INSTITUTO POLITÉCNICO DE BEJA

Escola Superior de Tecnologia e Gestão

Mestrado em Engenharia de Segurança Informática

Proposta de plataforma para o ensino de técnicas de hacking em ambiente de laboratório virtualizado, baseada em tecnologias abertas e de baixo custo

Vitor Manuel Sousa Farropas

Beja

2015

INSTITUTO POLITÉCNICO DE BEJA

Escola Superior de Tecnologia e Gestão

Mestrado em Engenharia de Segurança Informática

Proposta de plataforma para o ensino de técnicas de hacking em ambiente de laboratório virtualizado, baseada em tecnologias abertas e de baixo custo

Dissertação de mestrado apresentada na Escola Superior de Tecnologia e Gestão do Instituto Politécnico de Beja

Elaborado por:

Vitor Manuel Sousa Farropas

Orientado por:

Doutor Rui Miguel Soares Silva

Beja

2015

Resumo

Esta dissertação apresenta, de uma forma enquadrada, a implementação de uma solução prática para o ensino de técnicas de *hacking*.

Esta consiste no desenvolvimento de uma plataforma, de baixo custo, para o ensino dessas técnicas de ataque a sistemas informáticos, estruturada do ponto de vista pedagógico e capaz de suportar cenários com topologias variadas.

Os ambientes e cenários permitem aos alunos e professores explorar os sistemas, ferramentas, vulnerabilidades e *exploits*, orientados para o ensino e aprendizagem. Esta orientação é sustentada com um conjunto de arquiteturas de sistemas que permitem, de forma faseada, a integração, implementação e crescimento da solução desde a sala de aula até ao ensino à distância.

Palavras-chave

Ensino, *hacking*, cibersegurança, técnicas de *hacking*, plataforma de ensino, ensino à distância.

Abstract

This thesis presents a framed form, the implementation of a practical solution for teaching hacking techniques.

The platform was developed, with a low cost, for teaching these techniques to attack computer systems, structured from a pedagogical point of view and able to withstand scenarios with varying topologies.

The environments and scenarios allow students and teachers to explore the systems, tools, vulnerabilities and exploits, oriented to educational and learning purpose. This guidance is supported with a set of architectural systems that allow integration, implementation and growth of the solution, in a phased manner, from the classroom to distance learning.

Key words

Teaching, hacking, cyber security, hacking techniques, teaching platform, distance learning.

«...sempre em frente, sempre mais alto!»

Agradecimentos

À Minha Família, em especial aos meus filhos, Mariana e João Maria, à minha companheira e esposa, Alda Delfino, um enorme obrigado por acreditarem sempre em mim e naquilo que faço e por todos os ensinamentos de vida. Espero que esta etapa, que agora termino, possa, de alguma forma, retribuir e compensar todo o carinho, apoio e dedicação que, constantemente, me oferecem. A eles, dedico todo este trabalho!

Ao Coordenador do Mestrado em Engenharia de Segurança Informática e meu orientador, Doutor Rui Miguel Soares Silva, e aos Professores, agradeço a oportunidade e o privilégio que tive em frequentar este Mestrado que em muito contribuiu para o enriquecimento da minha formação académica e científica.

Aos meus companheiros do Mestrado em Engenharia de Segurança Informática e a todas as pessoas que, no decorrer do mesmo me ajudaram, direta ou indiretamente, a alcançar e cumprir os objetivos e a realizar com sucesso mais esta etapa da minha formação académica.

Índice Geral

Índice de figuras

Índice de gráficos

Lista de abreviaturas e siglas

Segue-se a lista de abreviaturas e siglas utilizadas ao longo desta dissertação, pretendendo-se assim, simplificar a sua leitura.

$(ISC)^2$ ou (ISC)2 - International Information System Security Certification Consortium

CAPEC – Common Attack Pattern Enumeration and Classification

CBK – Common Body of Knowledge

CEH – Certified Ethical Hacker

CERT – Computer Emergency Response Team

CERT/CC – Computer Emergency Response Team Coordination Center

CISSP – Certified Information Systems Security Professional

CNCS – Centro Nacional de Cibersegurança

CPE – Continuing Professional Education

CPU – Central Processing Unit

CSIRT – Computer Security Incident Response Team

CTF – Capture The Flag

CTP – Cracking the Perimeter

CVE – Common Vulnerabilities and Exposures

CWE – Common Weakness Enumeration

EaD – Ensino à Distância

EC-C ou EC-Council – International Council of Electronic Commerce Consultants

ENISA – European Network and Information Security Agency

GIAC – Global Information Assurance Certification

GSE – GIAC Security Expert

GSEC – GIAC Security Essentials

GUI – Graphical User Interface

ISSAP – Information Systems Security Architecture Professional

ISSEP – Information Systems Security Engineering Professional

ISSMP – Information Systems Security Management Professional

NIST – National Institute of Standards and Technology

OS - Offencive Security

OSCE – Offensive Security Certified Expert

OSCP – Offensive Security Certified Professional

OSEE – Offensive Security Exploitation Expert

OSWE – Offensive Security Web Expert

OSWP – Offensive Security Wireless Professional

PWK – Penetration Testing with Kali Linux

RAM – Randmon Access Memory

SANS – SysAdmin, Audit, Networking, and Security

SFP – Small Form-factor Pluggable transceiver

SFP+ - Enhanced Small Forma-factor Pluggable transceiver

UE – União Europeia

VERDICT – Validation Expousure Randomness Deallocation Improper Conditions Taxonomy

VLAN – Virtual Local Area Network

VM ou VMs – Virtual Machine ou Máquina Virtual

VPN – Virtual Private Network

WiFu – Offensive Security Wireless Attacks

INTRODUÇÃO

Neste capítulo serão abordados os assuntos relacionados com a motivação para esta dissertação e estrutura do documento de trabalho a desenvolver.

1 Introdução

O conhecimento de técnicas de ataque é um requisito para melhor defender. Neste domínio os sistemas informáticos não são diferentes. A natureza prática desta área obriga a um conhecimento prático efetivo de "como se faz" e de "mãos na massa" para poder proteger objetivamente e com a eficácia necessária. Esta é a abordagem que tem sido seguida no Mestrado de Engenharia de Segurança Informática do Instituto Politécnico de Beja. Esta é a grande motivação para a criação de uma plataforma de ensino desta natureza. É com uma ferramenta de aprendizagem que permita compreender, estudar, analisar e reconhecer os ataques que se pode preparar a defesa dos dados e informações. A segurança ofensiva tem nas suas componentes o conhecimento especializado dos ataques para melhor proteger, e parece-nos ser o caminho para formar melhores especialistas nesta matéria.

Por um lado este assunto está na ordem do dia nas notícias e conversas sobre dados e segurança, acessos indevidos e roubo de informação, por outro temos de aprender a executar esses ataques para melhor os compreender, estudar, analisar e reconhecer.

A quantidade de cenários a incluir numa plataforma desta natureza é enorme, sendo que, neste caso concreto, a quantidade não é sinónimo de qualidade. Os cenários a implementar devem permitir, de forma progressiva e estruturada, uma aprendizagem sustentada quer ao nível dos conhecimentos adquiridos, quer ao nível do que são as técnicas mais utilizadas em ataques informáticos e da sua prática.

O processo de escolha da plataforma e dos cenários a implementar deve ter por base um entendimento da globalidade dos ataques informáticos, caracterizando-os e classificando-os de acordo com um entendimento o mais alargado possível para permitir o seu ensino. Existem diversas taxonomias e classificações de ataques informáticos que devem servir de base à análise dos cenários que permitam a construção progressiva de uma biblioteca estruturada para o ensino de técnicas de *hacking* e para uma boa aprendizagem dessas mesmas técnicas de ataque a sistemas informáticos.

O propósito desta dissertação consiste no desenvolvimento de uma plataforma, de baixo custo, para o ensino dessas técnicas de ataque a sistemas informáticos, estruturada do ponto de vista pedagógico e capaz de suportar cenários com topologias variadas.

O restante documento está organizado em sete capítulos e um apêndice.

O capítulo 2 faz o enquadramento e estado a arte no que respeita à formação e certificação que são a referência atual nesta área de formação. São ainda apresentadas outras soluções não formais de ensino, como contributo formativo no ensino das técnicas de hacking e formula-se a hipótese de investigação.

O capítulo 3 mostra as tecnologias de virtualização que, no momento, estão em maior utilização no mercado, procedendo-se à escolha da tecnologia a usar na implementação face à hipótese de investigação que norteia este trabalho.

O capítulo 4 apresenta as considerações e exemplos dos regimes de ensino, cenários de utilização, trabalhos e avaliações da plataforma de ensino de técnicas de *hacking* a desenvolver.

O capítulo 5 aborda a plataforma de ensino desenvolvida, caracterizando diferentes cenários de arquitetura, a sua utilização e crescimento, parametrizações efetuadas, atividades de gestão e alguns automatismos para o uso da plataforma.

O capítulo 6 apresenta as taxonomias e classificações de ataques, conceitos e instituições envolvidas neste processo e apresenta um possível protótipo de módulo de ensino.

O capítulo 7 mostra a avaliação da plataforma proposta, analisa o seu desempenho e formula algumas considerações sobre a mesma.

O capítulo 8 apresenta as conclusões do trabalho desenvolvido e refere aspetos a melhorar no futuro.

O Apêndice 1 apresenta um manual de apoio ao aluno e professor para ajudar na configuração técnica dos seus computadores no acesso à plataforma de ensino.

ESTADO DA ARTE E HIPÓTESE DE INVESTIGAÇÃO

Neste capítulo serão abordados os assuntos relacionados com o estado da arte na formação e ensino de técnicas de *hacking*, com e sem, certificação e é formulada a hipótese de investigação para esta dissertação.

2 Estado da Arte e Hipótese de Investigação

Com as notícias crescentes sobre ameaças aos dados, redes e cibersegurança as certificações e certificadores também crescem. São apontadas algumas das que são consideradas de referência nesta área, quer ao nível empresarial, quer ao nível particular, nomeadamente: International Information System Security Certification Consortium (ISC)^2 [1], Offencive Security [2], SANS Technology Institute [3] e EC-Council [4], enquanto certificações formais e de referência no mercado empresarial; e um leque variado de sites que agrupam e apresentam diferentes produtos e máquinas virtuais para uma certificação/formação "não formal".

As secções seguintes deste capítulo abordam a formação com certificação, cursos e certificações de referência no mercado, formação não formal e formulação da hipótese de investigação desta dissertação.

2.1 Formação com certificação

A formação certificada é uma referência ao nível empresarial, dado que permite às empresas e profissionais que trabalham em cibersegurança e segurança da informação mostrar aos seus clientes que contratam profissionais à altura dos desafios e necessidades dos nossos dias.

As certificações disponíveis, a este nível, são diversas e de diferentes características, no entanto, podem-se identificar quatro das que são de referência à dimensão mundial:

- International Information System Security Certification Consortium (ISC)^2 [1];
- Offencive Security [2];
- SANS Technology Institute [3];
- EC-Council [4].

As certificações apresentadas por estas instituições têm em alguns casos um prazo de validade, precisando ser renovadas periodicamente. Estas renovações, como é o caso da (ISC)^2, têm de ser feitas em períodos de três anos, e passam pelo pagamento de um

valor de manutenção anual acrescido de uma acreditação de 120 créditos (CPE – *Continuing Professional Education*) por três anos. Estas unidades de créditos apresentam algumas correspondências entre as diferentes certificações que cada empresa/instituição ministra, nomeadamente, uma certificação da Offensive Security pode atribuir 40 créditos CPE para a renovação da certificação $(ISC)^2$, apesar desta correspondência, existem CPE que não têm correspondência com nenhuma outra certificação e são apenas medida dentro das certificações da própria empresa/instituição, como é o caso do SANS Technology Institute.

2.1.1 International Information System Security Certification Consortium, Inc. $(ISC)^2$

O $(ISC)^2$ [1] é uma instituição sem fins lucrativos com presença em todo o mundo ao nível da educação, formação e certificação de profissionais em segurança da informação.

É umas das instituições de maior referência nesta área, e, na sua estrutura de formação (CBK – *Commom Body of Knowledge*) encontramos domínios que abrangem desde a cibersegurança, segurança da informação, legislação e regulamentação, risco e gestão do risco, proteção e segurança de ativos, design e segurança de redes, controlo de acessos e gestão de identidades, design, realização e análise de testes de segurança e penetração, gestão de incidentes, segurança de software, comunicações e segurança de redes, *disaster recovery* à criptografia.

2.1.1.1 Certified Information Systems Security Professional – CISSP

Esta certificação, CISSP, foi desenhada de maneira a que os profissionais de segurança da informação possam, de uma forma simples, atualizada e global, atingir um conhecimento profundo e detalhado sobre novas ameaças, tecnologias, regulamentos, *standards* e práticas.

Para que se possa realizar o exame de certificação são necessários cinco anos de experiência em dois dos oito domínios da prova. Este exame apresenta um total de 250 perguntas de escolha múltipla, que têm de ser respondidas em 6 horas, e para obter aprovação tem que se responder corretamente a 700 ou mais pontos da prova. O seu custo de realização é de 520 EUR / 599 USD.

Após a conclusão do processo de certificação, o $(ISC)^2$ seleciona aleatoriamente, de entre os candidatos aprovados, um conjunto para serem auditados, e terem assim uma medida de qualidade das competências e validade das certificações.

2.1.1.1.1 Information Systems Security Architecture Professional - CISSP-ISSAP

A CISSP-ISSAP é uma certificação que está vocacionada para profissionais que ocupam cargos de chefia, nomeadamente nas áreas de arquitetura e implementação de programas e soluções de segurança da informação.

Para se poder candidatar ao exame é preciso ter a certificação CISSP e um mínimo de dois anos de experiência num dos seis domínios da prova. Este exame tem 125 perguntas de escolha múltipla com 3 horas para a sua conclusão, e para obter aprovação tem que se responder corretamente a 700 ou mais pontos da prova. O seu custo de realização é de 350 EUR / 399 USD.

Da mesma forma que na certificação CISSP, após a conclusão do processo de certificação, de entre os candidatos aprovados, é selecionado um conjunto para serem auditados, e desta forma aferir a qualidade das competências e certificações.

2.1.1.1.2 Information Systems Security Engineering Professional - CISSP-ISSEP

Esta certificação, CISSP-ISSEP, está direcionada para as metodologias e boas práticas que podem ser utilizadas para a integração da segurança nas diferentes fases de implementação dos sistemas de informação. Aborda a integração de standards e metodologias em áreas como a gestão do risco, engenharia de segurança de sistemas, certificação e acreditação.

À semelhança da certificação anterior, para se poder candidatar ao exame é preciso ter a certificação CISSP e um mínimo de dois anos de experiência num dos seis domínios da prova. Este exame tem 150 perguntas de escolha múltipla com 3 horas para a sua conclusão, e para obter aprovação tem que se responder corretamente a 700 ou mais pontos da prova. O seu custo de realização é de 350 EUR / 399 USD.

De igual forma que na certificação ISSAP, após a conclusão do processo de certificação, os candidatos aprovados, podem ser selecionados para serem auditados, e assim aferir a qualidade das competências e certificações.

2.1.1.1.3 Information Systems Security Management Professional - CISSP-ISSMP

A certificação, CISSP-ISSMP, está vocacionada para a liderança e governância da informação e dos sistemas de informação. Tipicamente estes profissionais são responsáveis pela construção e gestão de *frameworks* para os departamentos de segurança da informação das instituições.

Esta certificação encerra a concentração CISSP, e apresenta condições semelhantes às ISSAP e ISSEP, para se poder candidatar ao exame é preciso ter a certificação CISSP e um mínimo de dois anos de experiência num dos seis domínios da prova. Este exame tem 125 perguntas de escolha múltipla com 3 horas para a sua conclusão, e para obter aprovação tem que se responder corretamente a 700 ou mais pontos da prova. O seu custo de realização é de 350 EUR / 399 USD.

Igualmente, à semelhança das anteriores, estes candidatos aprovados podem ser auditados como medida da qualidade das competências e certificações.

2.1.2 Offensive Security

A empresa Offensive Security [2] fundou e mantem os projetos *Kali Linux* [5], *Exploit Database* [6] e *metasploit unleashed* [2]. Na formação tem certificações e cursos em segurança ofensiva e em ambiente controlado. Para obter a certificação é necessário realizar a formação efetiva e obter aprovação no respectivo exame. De entre os cursos mais relevantes estão o Penetration Testing with Kali Linux (PWK), Offensive Security Wireless Attacks (WiFu) e Cracking the Perimeter (CTP), que permitem o acesso às certificações Offensive Security Certified Professional (OSCP), Offensive Security Wireless Professional (OSWP), Offensive Security Certified Expert (OSCE), Offensive Security Exploitation Expert (OSEE) e Offensive Security Web Expert (OSWE).

Conforme referido anteriormente, a frequência e aprovação, dos cursos e certificações da Offensive Security, têm uma equivalência de créditos CPE que podem ser usados, por exemplo na renovação das certificações do $(ISC)^2$.

2.1.2.1 Offensive Security Certified Professional – OSCP

Esta certificação caracteriza-se por ser do tipo "mãos na massa", desafiando os alunos a provar que têm um conhecimento prático do processo e ciclo de vida dos testes de penetração durante as 24 horas do exame de certificação.

Para poder realizar o exame de certificação é necessário o curso Penetration Testing with Kali Linux (PWK), que está disponível por 90 dias, após o seu início. Neste curso os alunos adquirem as competências para a realização do exame. Uma vez concluído o curso, o exame de certificação apresenta-se de forma progressiva e durante 24 horas de duração. Para ser aprovado o candidato tem de submeter um Relatório do Teste de Penetração realizado, contendo, notas e capturas de ecrã que documentem a suas descobertas sobre as máquinas, infraestrutura de rede, sistemas e aplicações. A cada descoberta documentada, e de acordo com a sua dificuldade, serão atribuídos pontos. Esta certificação tem um custo de 1020 EUR / 1150 USD.

Após a sua conclusão, com aprovação, tem a correspondência de 40 créditos CPE, por exemplo para a renovação da certificação do $(ISC)^2$.

2.1.2.2 Offensive Security Wireless Professional – OSWP

Esta certificação centra-se na indústria *wireless* de forma a organizar e resumir os ataques Wi-Fi relevantes, fornecendo uma sólida compreensão das vulnerabilidades e fragilidades sobre as redes e equipamentos sem fios.

Para poder realizar o exame de certificação é preciso o curso Offensive Security Wireless Attacks (WiFu), que está disponível por 120 dias. Neste curso os alunos adquirem as competências para a realização do exame. O exame de certificação apresenta-se de forma progressiva e tem 4 horas de duração. Para ser aprovado o candidato tem de ultrapassar todas as etapas práticas do exame e recuperar as chaves encriptadas em uso na rede wireless, explorando as diferentes vulnerabilidades que encontre. Esta certificação tem um custo de 399 EUR / 450 USD.

Depois da sua conclusão, com sucesso, tem a correspondência de 10 créditos CPE, por exemplo para a renovação da certificação do $(ISC)^2$.

2.1.2.3 Offensive Security Certified Expert – OSCE

A OSCE é uma certificação de *ethical hacking*, está desenhada para que se ganhem competências que permitam ultrapassar com sucesso o Cracking the Perimeter (CTP). É um curso projetado no formato "mãos na massa" para profissionais de testes de penetração de nível avançado.

Para poder realizar o exame de certificação o aluno frequenta o curso Cracking the Perimeter (CTP), que está disponível por 60 dias, após o seu início. Neste curso os alunos adquirem as competências para a realização do exame de certificação. Este apresenta-se de forma progressiva e durante 48 horas de duração. Para ser aprovado o candidato tem de demonstrar, num cenário real, em ambiente controlado, que adquiriu e tem conhecimentos avançados na identificação de vulnerabilidades e na sua exploração, mostrando assim as suas competências em testes de penetração de nível avançado. Esta certificação tem um custo de 1335 EUR / 1500 USD.

Uma vez terminada com aprovação esta certificação tem a correspondência de 40 créditos CPE , por exemplo para a renovação da certificação do $(ISC)^2$.

2.1.2.4 Offensive Security Exploitation Expert – OSEE

Esta certificação está vocacionada para o desenvolvimento de *exploits*, em especial para Sistemas Windows, obtendo-se competências para a documentação e desenvolvimento de *exploits*.

Para poder realizar o exame de certificação é necessário o curso Advanced Windows Exploitation (AWE), que é em regime presencial. Neste curso os alunos adquirem as competências para a realização do exame. Uma vez concluído o curso, o exame de certificação apresenta-se de forma progressiva e durante 72 horas de duração. Para ser aprovado o candidato tem de aceder ao ambiente de laboratório virtual, onde está configurado um número limitado de sistemas de destino que contêm o software com as vulnerabilidades específicas e desconhecidas para as quais o aluno deve desenvolver os *exploits*, documentando de forma integral todas as medidas que foi tomando. Esta certificação tem sido ministrada no decorrer de conferências como a Black Hat USA 2015, uma vez que é necessário um acompanhamento presencial dos

alunos. É ainda possível que às empresas, constituindo um grupo turma, possam requerer este curso e certificação. Os custo envolvidos dependem do grupo turma.

Com esta certificação o aluno tem a correspondência de 40 créditos CPE, por exemplo para a renovação da certificação do $(ISC)^2$.

2.1.2.5 Offensive Security Web Expert – OSWE

Esta certificação está centrada nos testes de penetração para aplicações *web*, tendo também a característica de "mãos na massa" e permite adquirir conhecimentos ao nível da *web* e dos seus processos.

Para poder realizar o exame de certificação é necessário o curso Advanced Web Attacks and Exploitation (AWAE), que é em regime presencial. Neste curso os alunos adquirem as competências para a realização do exame. Uma vez concluído o curso, o exame de certificação apresenta-se de forma progressiva e durante 24 horas de duração. Para ser aprovado o candidato tem de aceder ao ambiente de laboratório virtual, e adquirir privilégio de administração nos sistemas da rede em estudo, documentando de forma integral todas as medidas que foi tomando. Esta certificação, à semelhança da anterior, tem sido ministrada no decorrer de conferências como a Black Hat USA 2015, uma vez que é necessário um acompanhamento presencial dos alunos. É ainda possível que às empresas, constituindo um grupo turma, possam requerer este curso e certificação. Os custo envolvidos dependem do grupo turma.

Com esta certificação o aluno tem a correspondência de 40 créditos CPE, por exemplo para a renovação da certificação do $(ISC)^2$.

2.1.3 SANS Technology Institute

O SANS Technology Institute [3] é uma empresa privada especializada na formação em segurança da informação e cibersegurança. Considerada como uma das maiores fontes de formação de segurança da informação e de certificação de segurança no mundo.

Desenvolve, mantém e disponibiliza, gratuitamente, uma grande biblioteca de documentos sobre vários aspetos da segurança da informação. Esta informação é depois utilizada no processo de educação/treino do SANS Technology Institute [3] e certificação através da Global Information Assurance Certification [7].

Estas certificações usam um sistema de créditos CPE num máximo de 36 por curso e certificação, no entanto não têm correspondência com outros sistemas de créditos existentes, como os que já foram referidos anteriormente.

No caso das renovações de certificação com recurso a CPE, é possível usar os cursos de treino do SANS, com a atribuição de 1 crédito CPE por hora de curso, através da publicação de livros, artigos ou *papers*, cursos de outras instituições até um máximo de 12 CPE ou experiência profissional com 6 CPE por ano, até um máximo de 12. Todos estes CPE têm de ser devidamente comprovados e documentados, e ainda, submetidos nos 2 ou 3 anos antes de terminar o prazo da certificação SANS que se pretende renovar que se encontra nos 4 anos.

2.1.3.1 GIAC Security Essentials – GSEC

É uma certificação destinada a profissionais que estão qualificados e que têm experiência, na e para, segurança de sistemas de tecnologias da informação. Esta certificação não obriga a nenhum treino específico no Instituto, apenas a aprovação do exame, que se apresenta com um total de 180 perguntas, com o máximo de 5 horas para completar as respostas, e para obter aprovação tem de responder corretamente a um mínimo de 74%. Esta certificação tem um período de validade de 4 anos e antes do seu término tem de ser renovada para que os profissionais continuem a ser reconhecidos pelo SANS.

O custo de realização é de 559 EUR / 629 USD, no caso de adquirir a formação no SANS Technology Institute. Caso queira apenas o exame de certificação este terá um custo de 977 EUR / 1099 USD.

Com esta certificação o aluno tem os 36 créditos CPE necessários para a renovação da certificação, por mais 4 anos, do SANS Technology Institute.

2.1.3.2 GIAC Security Expert – GSE

Esta certificação é apresentada como a certificação mais prestigiada no sector das tecnologias da informação e segurança. É do tipo "mãos na massa" e está dividida em duas partes. A parte 1 é um exame de escolha múltipla, cuja aprovação, com um mínimo de 75%, e 3 horas de duração, permite a passagem à parte 2. Esta qualifica o

profissional para a entrada no laboratório GSE, com a duração de 18 meses. Este processo termina com o exame de dois dias sobre o laboratório, que inclui cenários de resposta a incidentes, análise de dados e resultados, relatórios técnicos, e, todo um conjunto de exercícios de carácter prático sobre os domínios estudados no laboratório GSE. Esta certificação tem um período de validade de 4 anos e antes do seu término tem de ser renovada para que os profissionais continuem a ser reconhecidos pelo SANS.

Os custos envolvidos para a certificação GSE são de 355 EUR / 399 USD para a parte 1, e de 1778 EUR / 1999 USD para o laboratório.

Para continuar certificado é preciso realizar e aprovar, a cada 4 anos, o exame de certificação parte 1. Com esta certificação o SANS renova também todas as certificações GIAC do candidato.

2.1.4 EC-Council

O International Council of Electronic Commerce Consultants (EC-Council) [4] tem como propósito o suporte e apoio aos indivíduos e organizações que desenham, criam, gerem ou comercializam soluções de *e-business* e de segurança e cibersegurança. Os programas de treino e apoio para a certificação são ministrados por diversas instituições no mundo inteiro.

2.1.4.1 Certified Ethical Hacker – CEH

O CEH é uma certificação que é abrangente, ao nível do *Ethical Hacking*, a Segurança de Sistemas de Informação e Auditoria, com foco em ameaças de segurança recentes, vectores de ataque avançados, é prático e com demonstração, em tempo real, das últimas técnicas de *hacking*, metodologias, ferramentas, truques e medidas de segurança.

O laboratório, de cinco dias, do tipo "mão na massa", permite adquirir um profundo conhecimento e experiência prática sobre a segurança de sistemas de informação. Esta formação prepara para a realização do exame de certificação do EC-Council CEH 312-50.

Antes da realização da prova o candidato tem de submeter o pedido de idoneidade para verificação. O exame tem um total de 125 perguntas de escolha múltipla para serem respondidas em 4 horas, e para aprovar é necessário um mínimo de 70% de respostas corretas.

O custo associado da formação e exame desta certificação é de 2570 EUR / 2895 USD que inclui a documentação oficial, acesso de 6 meses ao iLabs e exame de certificação.

No que se refere aos créditos CPE, o EC-Council, não apresenta, à data, um sistema de acreditação de competências.

2.2 Formação sem certificação

Existem, ainda que de forma "não formal" e sem certificação reconhecida, soluções de prática de técnicas de *hacking* com conteúdos multimédia que estão disponíveis para utilização *ha-doc*. Apesar de estas soluções não apresentarem uma certificação formal, não deixam de ser uma importante fonte de recursos, testes e exemplos para quem queira adquirir conhecimentos na área da cibersegurança e segurança da informação, testes de penetração, utilização de *exploits* e vulnerabilidades. Como exemplos destas fontes temos:

2.2.1 VulnHub

O site VulnHub [8] tem um conjunto de máquinas virtuais que permite que qualquer utilizador possa praticar "mãos na massa" em cenários de segurança, aplicações e administração e redes.

2.2.2 The Hacking Dojo

Este site, The Hacking Dojo [9], disponibiliza aos visitantes e alunos um conjunto de sistemas para treino com apoio e acesso a professores para apoio. Permite a aprendizagem sobre testes de penetração através de tutoriais vídeo.

2.2.3 Smash the Stack

O site Smash the Stack [10] tem um conjunto de "Jogos de Guerra" criando um ambiente de *ethical hacking*, simulando situações do mundo real, para treino sobre vulnerabilidades e técnicas de *hacking*.

2.2.4 Hack This Site

Este site, Hack This Site [11], é um sítio gratuito, que permite de forma segura e legal, treinar e aumentar os conhecimentos de *hacking*. Pretende ser mais do que um site de "Jogos de Guerra", e ser uma comunidade viva com projetos a serem desenvolvidos, artigos da especialidade e fóruns de apoio aos seus utilizadores.

2.2.5 OverTheWire

O site OverTheWire [12] é constituído por um grupo de voluntários que, no seu tempo livre, mantem o sistema e adiciona novos "Jogos de Guerra". Esta comunidade é suportada por patrocinadores, apoios e contribuições diversas, dos seus membros e voluntários.

2.3 Hipótese de Investigação

O ensino superior foca-se mais nos aspetos científicos dos sistemas e nas questões defensivas do que nos aspectos operacionais dos ataques aos sistemas, apesar de haver algumas instituições que têm uma abordagem mais ofensiva na formação dos seus alunos, como é o caso do Mestrado em Engenharia de Segurança Informática do Instituto Politécnico de Beja. O contributo desta dissertação vem no seguimento desta linha orientadora. Tendo em conta esta perspectiva formulou-se a seguinte proposta de investigação:

"É possível desenvolver uma plataforma para o ensino em ambiente de laboratório virtualizado, baseada em tecnologias abertas e de baixo custo, orientada para o ensino de técnicas de hacking em conformidade com as taxonomias vigentes, através de um conjunto de conteúdos multimédia, estruturados de forma pedagógica centrada na aprendizagem pela prática, que possibilite inclusivamente o ensino à distância?"

De acordo com a orientação ofensiva e de "mãos na massa" que o Mestrado em Engenharia de Segurança Informática abraça, esta proposta de plataforma para o ensino de técnicas de *hacking* em ambiente virtualizado pretende ir ao encontro das necessidades mais específicas que este desafio representa.

Ensinar e passar conhecimento é uma tarefa exigente, tanto maior quanto a especificidade das matérias a lecionar.

Procura-se, com esta dissertação, implementar um modelo que possa dar respostas não só às necessidades técnicas, mas também às pedagógicas. No caso destas últimas, é importante termos uma abordagem igualmente de "mãos na massa" para que se consigam alcançar os objectivos práticos e consolidar os conhecimentos e compreensão das matérias envolvidas.

É sobre estas necessidades pedagógicas que se centra esta dissertação, não descuidando a sua relação com as componentes práticas do *hacking*, bem como, a sua interligação com o mundo real.

Analisando, de uma forma mais estruturada, a hipótese de investigação apresentada podemos considerar um conjunto de aspectos que ajudam a compreender melhor as opções tomadas ao longo da dissertação. Assim, temos:

1. Plataforma de ensino – criar uma plataforma de ensino, usando um servidor de virtualização que permita virtualizar os ambientes e cenários a implementar, sejam criados ou resultantes da virtualização de máquinas reais.
2. Tecnologia aberta – analisar as diferentes tecnologias de virtualização e escolher a que seja mais adequada à hipótese de investigação.
3. Tecnologia de baixo custo – analisar os custos de licenciamento, ou não, e utilização das diferentes tecnologias de virtualização e escolher a que seja mais adequada à hipótese de investigação.
4. Ensino de técnicas e competências – implementar e criar a estrutura funcional que permita a criação e o desenvolvimento dos cenários desejados para o ensino e aprendizagem das técnicas de *hacking*.

5. Taxonomias vigentes – face às taxonomias vigentes, entre elas o *Common Attack Pattern Enumeration and Classification* (CAPEC), propor um curriculum adequado ao ensino e aprendizagem das técnicas de *hacking*.
6. Conteúdo para o ensino – desenvolver e permitir a criação de cenários, para uso na plataforma, com conteúdos para o ensino e aprendizagem das técnicas de *hacking*.
7. Estrutura pedagógica centrada na prática – cada cenário desenvolve componentes que têm a possibilidade de virtualizar os ambientes reais. Este aspecto, apesar de não ser o único, é importante para os profissionais em formação nesta área, uma vez que a virtualização de cenários reais, e, a partir de cenários reais, dá um suporte e conhecimento prático sobre o que se passa no dia a dia. Por outro lado, em termos pedagógicos, esta prática real, permite o estudo e conhecimento dos casos reais, o que proporciona uma aprendizagem de compreensão e crescimento de conhecimentos que ultrapassa o fazer pela lista, isto é, os alunos realmente consolidam as aprendizagens teóricas com a prática e ficam com um conhecimento alargado sobre os problemas abordados.
8. Ensino à Distância – ligação por *Virtual Private Network* (VPN) à rede da Instituição de Ensino com o fim de permitir o uso à distância da plataforma, integrando as tecnologias já existentes neste âmbito, nomeadamente, o *moodle* [13] que já se encontra em utilização e serve de suporte às aulas e à distribuição de conteúdos pedagógicos. Para o ensino à distância a integração destas plataformas é o complemento para que os alunos possam, no seu ritmo e horário, aceder a todos os conteúdos, teóricos e práticos, em matéria de ensino de técnicas de *hacking*.

TECNOLOGIAS DE VIRTUALIZAÇÃO

Neste capítulo serão abordados os assuntos relacionados com as diferentes tecnologias de virtualização existentes mas com uma abordagem genérica. Escolha da tecnologia a usar nesta dissertação.

3 Tecnologias de virtualização

As tecnologias de virtualização não são novidade, e, não é o propósito deste trabalho detalhar exaustivamente as diferentes tecnologias existentes. De uma forma condensada, pode dizer-se que estas tecnologias permitem um controlo e uma descida dos custos associados aos equipamentos e seu funcionamento, permitindo que as instituições e empresas possam melhorar, escalar e flexibilizar os sistemas de tecnologias de informação através da virtualização dos seus sistemas e serviços.

No âmbito deste trabalho, tendo em conta a hipótese de investigação apresentada e a necessidade de virtualizar sistemas, é importante termos de uma forma genérica, o conhecimento de quais as que existem e são mais utilizadas para servidor, nomeadamente, VMWare vSphere [14], Microsoft Hyper-V Server [15], Citrix XenServer [16] e Proxmox VE [17], e que possam ser usadas para o desenvolvimento de plataformas e ambientes para o ensino e formação de pessoas.

De acordo com [17] a comparação das diferentes versões de software, para servidor, indicam que o Proxmox Virtual Environment, preenche os requisitos da hipótese de investigação, nomeadamente, ser *open source*, de baixo custo, gestão centralizada numa consola única e em ambiente gráfico, alta disponibilidade dos sistemas, *live snapshot* das máquinas virtuais, *backup* e migração sem parar as máquinas virtuais em execução, recaindo sobre ela a escolha de utilização para esta dissertação.

Dada a sua relevância, ao nível da virtualização de sistemas, são referidas duas outras soluções, que apesar de não serem para servidor, permitem a utilização pessoal de máquinas virtuais para o ensino de técnicas de *hacking*, nomeadamente: Oracle VirtualBox [18] e VMWare Player [19].

As secções seguintes deste capítulo abordam as diferentes tecnologias de virtualização existentes mas com uma abordagem genérica.

3.1 VMWare vSphere

Esta ferramenta da VMWare para servidor é uma das soluções implementada no mercado empresarial da virtualização [20]. A empresa proprietária desta tecnologia apresenta uma solução integrada e com um conjunto de ferramentas adicionais que permitem uma melhoria efetiva da solução, no entanto, e para o trabalho a desenvolver no âmbito desta dissertação apresenta um conjunto de características que não permitem a sua escolha, nomeadamente, os custos da solução e ferramentas adicionais.

3.2 Microsoft Hyper-V Server

Esta solução para servidor, proprietária da Microsoft, permite a instalação dos sistemas windows e alguns sistemas linux [21]. Não sendo uma solução de baixo custo, dado que implica o pagamento de licenciamento, observou-se ser uma das soluções implementadas ao nível empresarial, à semelhança de outros produtos da mesma empresa. Dado que existem algumas limitações ao nível dos sistemas que permitem e têm custos de software, esta solução, apesar de muito usada ao nível empresarial, não preenche os requisitos para esta dissertação.

3.3 Citrix XenServer

O produto da Citrix, apresenta-se como um solução para servidor que permite a virtualização da maioria dos sistemas operativos. Esta é igualmente uma das ferramentas de virtualização usada no mercado empresarial da atualidade [22]. Apesar de baseada em tecnologia *open source* tem custos de licenciamento associados e está ainda focada no mercado de *cloud*. Motivos pelos quais não vai ao encontro do tipo de produto para servidor que se procura no âmbito desta dissertação.

3.4 Proxmox VE

Esta solução de servidor de virtualização *open source*, com sistema de gestão completo, permite a virtualização dos sistemas Windows e Linux nas suas diversas

distribuições. Apresenta uma solução que permite um crescimento na medida das necessidades ao nível da virtualização de sistemas informáticos [23,24]. Tem uma comunidade de desenvolvimento e suporte muito ativa o que garante que a solução de eventuais problemas detetados sejam rapidamente resolvidos. Conforme referido, e pelos motivos apontados, esta foi a solução de software pela qual se optou para o trabalho desta dissertação.

3.5 Oracle VirtualBox

O Oracle VM VirtualBox é um *software* de virtualização multiplataforma que pode ser instalado em qualquer sistema com arquitetura Intel ou AMD, com sistema operativo Windows, Mac ou Linux [25]. Não sendo uma versão para servidor de virtualização, é muito utilizada para virtualizar sistemas em computadores pessoais dado ser uma solução que não apresenta custos e permite a virtualização de sistemas operativos windows e linux.

3.6 VMWare Player

O VMWare Player é uma solução de virtualização da VMWare que permite, no seu computador pessoal, fazer o *play* ou correr máquinas virtuais [19]. Possibilita a execução dos sistemas operativos mais comuns, mas apenas o *player* é gratuito, isto é, as versões do software, da VMWare, que permitem a criação de máquinas virtuais têm custos de licenciamento.

CARACTERIZAÇÃO DE ATIVIDADES LETIVAS

Neste capítulo serão abordados os assuntos relacionados com atividades e regimes letivos, considerações sobre trabalhos e avaliações, exemplos de cenários de utilização, testes e certificações.

4 Caracterização de atividades letivas

No âmbito da plataforma para o ensino de técnicas de *hacking*, os aspectos pedagógicos são, entre outros, um dos elementos de vital importância na definição do modelo conceptual que se pretende implementar.

As atividades letivas são um dos aspectos que permitem a sua utilização. Desta forma temos de considerar, desde logo, o Ensino Presencial e o Ensino à Distância, sendo que para qualquer das duas situações seja possível a utilização idêntica da plataforma para o ensino de técnicas de *hacking*, mesmo que para isso seja complementado com o uso de outros recursos, como por exemplo o *moodle* [13].

O processo de ensino e aprendizagem que se quer atingir é o de dotar os alunos com um conjunto de conhecimentos teóricos e práticos, através do uso de cenários reais e do tipo "mãos na massa", para que treinem nos cenários, mas ao mesmo tempo possam estar preparados para novas situações e consigam dar-lhes resposta.

As secções seguintes deste capítulo abordam a caracterização das atividades letivas nas vertentes de regimes letivos, conteúdos e atividades em sala de aula, trabalhos e avaliação dos alunos.

4.1 Regimes letivos

Os conceitos de regimes letivos não são novos, nem se pretende reinventá-los. No entanto é um fator importante na estrutura de suporte às aprendizagens dos alunos e à própria plataforma de ensino de técnicas de *hacking*, uma vez que se pretende que esta plataforma dê resposta a estes cenários. Podem considerar-se três regimes letivos:

- regime de ensino presencial;
- regime de ensino à distância;
- regime de ensino misto.

Na realidade podemos, para simplificar, dizer que existem dois regimes dado que o regime de ensino misto acaba por ser uma mistura dos regimes presencial e à

distância. Para os casos do regime de ensino misto, podemos acrescentar, que se é possível localmente e à distância, então também o é no regime de ensino misto.

Este enquadramento é importante para a dissertação na medida em que importa definir a estrutura que suporta a utilização da plataforma de ensino de técnicas de hacking, e, acima de tudo, permita uma aprendizagem pela prática dos futuros alunos a usar a plataforma. É esta prática de "mãos na massa" que norteia este trabalho.

4.1.1 Regime de Ensino Presencial

O regime de ensino presencial, como ilustra a Figura 1, pressupõe a presença efetiva do aluno em sala, onde a sua presença é fundamental para as aprendizagens, assim como, a interação com o professor e restantes alunos, equipamentos e tecnologias. Aqui os alunos frequentam fisicamente as aulas, laboratórios e atividades localmente.

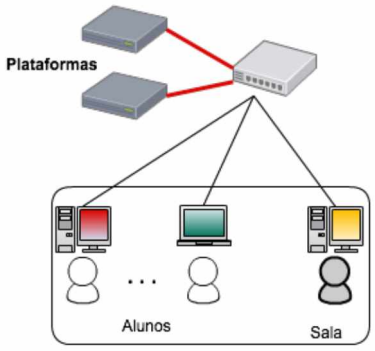


Figura 1 - Modelo de regime de ensino presencial

Da mesma forma que acontece em diferentes níveis de ensino, o uso de ferramentas de apoio às aulas como por exemplo o *moodle* [13], que permite a distribuição de trabalhos e fichas, a sua recepção/entrega, avaliação, bem como a distribuição de documentos e apontamentos aos alunos, integra o sistema de ensino e complementa a plataforma de ensino de técnicas de *hacking*. Coexistem e complementam-se enquanto ferramentas de ensino, e, esta última vem juntar-se para melhorar as aprendizagens dos alunos em técnicas de *hacking*.

4.1.2 Regime de Ensino à Distância

O regime de ensino à distância (EaD), ilustrado na Figura 2, é totalmente feito on-line, sejam sessões síncronas (todos os alunos com data e hora marcadas) ou assíncronas

(cada aluno no seu tempo) com recurso a uma plataforma de suporte às disciplinas, como por exemplo, o *moodle* [13].

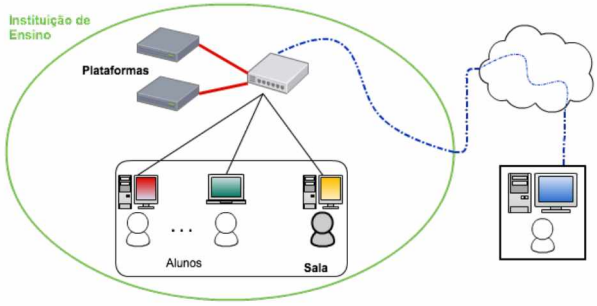


Figura 2 - Modelo de regime de ensino à distância

As sessões síncronas, obrigam a que seja marcada data e hora para o seu funcionamento, quer para o professor, quer para os alunos, isto é, todos os intervenientes no processo de ensino e aprendizagem têm de estar on-line ao mesmo tempo. Exemplos de atividades desta natureza são uma vídeo conferência, um *webcast live*, um teste de avaliação, ou um fórum interativo pergunta/resposta para tirar dúvidas.

Uma sessão assíncrona decorre no tempo de cada interveniente no processo de ensino e aprendizagem, isto é, o professor pode preparar uma atividade que cada aluno realiza na data e hora que mais lhe convém, podendo esta mesma atividade ter, ou não, data e hora para a sua conclusão por parte dos alunos. Exemplos de atividades assíncronas são um *webcast* gravado, um *podcast*, um fórum de apoio, documentação, entrega de fichas ou trabalhos, ou mesmo um vídeo didático.

A plataforma *moodle* [13] já está amplamente implementada no ensino, quer básico e secundário, quer no ensino superior, e permite este tipo de interação com os alunos.

Integrando e interagindo com este modelo existente, a plataforma de ensino de técnicas de *hacking*, propõe, em ambiente controlado, aprendizagens ao nível da segurança e cibersegurança em sistemas de informação e comunicação, onde os conteúdos práticos de experiências, testes, ensaios ou avaliações podem ser conduzidos.

A componente mais teórica de suporte, documentação ou fórum de apoio à formação prática, é apoiada no *moodle* [13]. Esta última plataforma *moodle* [13] já está a funcionar neste modelo na maioria das instituições de ensino superior.

4.1.3 Regime de Ensino Misto

O regime de ensino misto ou *B-Learning* (B = *blended*), integra uma solução equilibrada dado que permite sessões presenciais e sessões on-line, como se observa na Figura 3, sejam estas síncronas ou assíncronas.

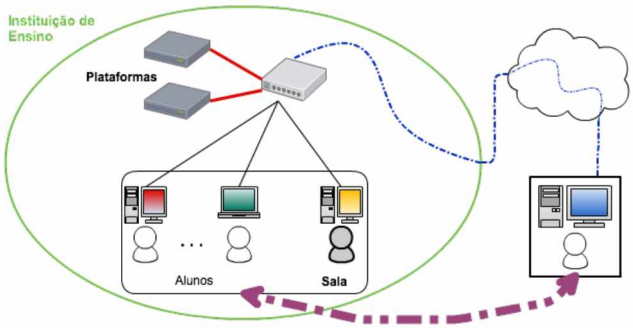


Figura 3 - Modelo de regime de ensino misto

Este modelo permite ao aluno fazer o seu estudo ao seu ritmo, isto é, pode assistir às aulas, tirar dúvidas com o professor presencialmente, e aceder ao ambiente da plataforma de ensino de técnicas de hacking no seu próprio horário, progredindo e consolidando as suas aprendizagens no seu próprio ritmo.

Existe uma mistura dos modelos presencial e à distância, permitindo ao aluno tirar o maior partido de cada regime, no sentido dos seus conhecimentos e aprendizagens. É, eventualmente, aqui que reside a mais valia desde modelo.

4.2 Sala de aula

A sala de aula, física ou virtual, é um espaço de ensinamentos e aprendizagem, troca de experiências, que nas áreas tecnológicas têm uma componente prática forte.

As diferentes implementações de salas de aula são possíveis nos regimes presencial e à distância. Pretende-se uma solução que seja transparente, quer para o aluno, quer para o professor, e nesta perspetiva é importante reforçar que os cenários de utilização apresentados são igualmente funcionais.

Na situação de sala de aula, virtual ou não, existem diferentes tipos de espaços para as aprendizagens, podendo distinguir-se os seguintes: aulas, laboratórios, testes, avaliações e certificações. Para compreender melhor estes conceitos, ao nível da plataforma para o ensino de técnicas de *hacking*, seguem-se três exemplos que ilustram algumas dessas aulas.

4.2.1 Cenário de utilização - aula

Este cenário de utilização da plataforma é o caso mais clássico de ensino, o professor está em sala e acompanha os alunos nas suas aprendizagens, explica e expõe, através de exemplos, a matéria teórica e prática necessária para a compreensão dos conteúdos apresentados.

No exemplo da Figura 4, os alunos estão em sala de aula e o professor está na sua área de trabalho da plataforma de ensino de técnicas de *hacking*, através da partilha da sua máquina virtual, permite o acesso ao seu ambiente de trabalho virtual para que os alunos possam acompanhar, nos seus ecrãs, a demonstração prática que o professor apresenta.

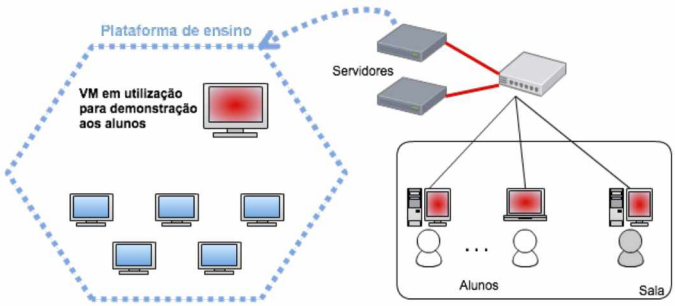


Figura 4 - Cenário 1 - regime de ensino presencial - AULA

Este cenário quando usado em regime presencial, permite uma interação mais imediata, e uma consolidação das aprendizagens pela prática, tal como referido anteriormente "mãos na massa". Esta abordagem, em termos de prática pedagógica, é também possível, com pequenas adaptações nas práticas do professor, nos restantes regimes, por exemplo com recurso a conversa on-line, fóruns, entre outros.

Um aluno em regime de ensino à distância, ligado à plataforma de ensino, pode estar a ver no seu ecrã, o ecrã do professor e acompanhar os passos que vão sendo demonstrados, as ferramentas utilizadas e os procedimentos usados.

No caso ilustrado na Figura 5, acontece ao mesmo tempo da aula, o que faz com que essa sessão seja síncrona, isto é, decorre no dia e hora da aula em sala.

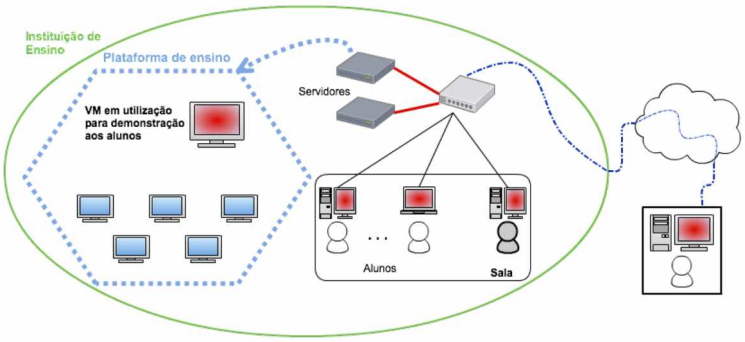


Figura 5 - Cenário 1 - regime de ensino à distância (sessão síncrona) - AULA

Para que possa haver uma interação com o professor e com os restantes alunos, é preciso que as "pequenas adaptações nas práticas pedagógicas do professor" façam com que esta aconteça.

O uso da plataforma *moodle* [13], como foi mencionado anteriormente, é disso exemplo, com um recurso de simples utilização como seja o fórum ou o *chat*, o aluno em regime de ensino à distância, tem um retorno imediato às suas dúvidas, sugestões e contributos para a sessão em que participa.

4.2.2 Cenário de utilização – laboratório

Neste cenário de utilização os alunos estão na sua área da plataforma de ensino de técnicas de *hacking*, com o seu conjunto de máquinas virtuais, e cada um na sua rede isolada, isto é, só existe comunicação entre as máquinas virtuais de cada aluno.

Um dos principais objetivos do cenário é permitir que cada aluno no seu ritmo e tempo possa experimentar, rever, testar e inovar nas suas aprendizagens individuais. Após ter assistido às aulas teóricas, revisto os seus apontamentos ou apreendido o material teórico que o professor facultou, cada aluno, consolida em laboratório as suas aprendizagens, e pode mesmo, encontrar situações novas às quais tem de se adaptar e ultrapassar.

Conforme ilustrado na Figura 6, fazendo esta sessão de laboratório em regime de ensino presencial, cada aluno pode de imediato tirar dúvidas com o professor em sala, ou mesmo trocar impressões com os restantes alunos.

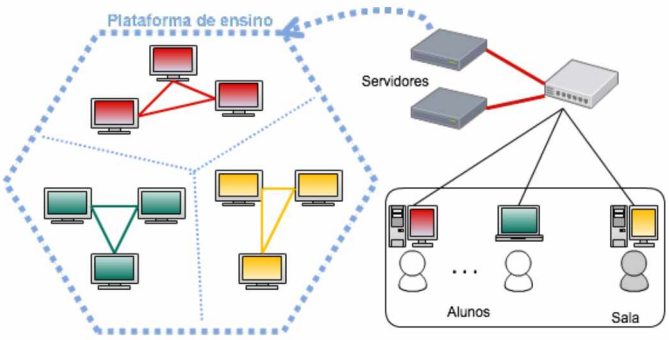


Figura 6 - Cenário 2 - regime de ensino presencial - LABORATÓRIO

Para o caso do aluno em regime de ensino à distância, as tarefas a realizar não diferem, isto é, após ter apreendido o material teórico disponibilizado pelo professor, o aluno progride ao seu ritmo nas matérias práticas de laboratório e consolida as suas aprendizagens, conforme mostra a Figura 7, à semelhança do que acontece com os alunos em regime de ensino presencial.

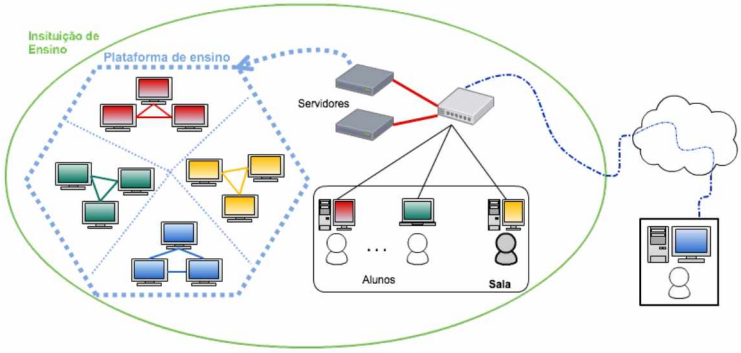


Figura 7 - Cenário 2 - regime de ensino à distância (sessão assíncrona) - LABORATÓRIO

As eventuais dúvidas que possam surgir serão ultrapassadas via fórum, *chat*, vídeo conferência, email ou outra forma de comunicação com o professor.

Uma vez que a comunicação com o professor se processa por vias que não implicam uma simultaneidade, estas sessões são assíncronas.

4.2.3 Cenário de utilização – teste / ctf

O uso da plataforma de ensino de técnicas de *hacking* com este cenário de utilização, permite o acesso concorrente dos alunos ao mesmo conjunto de máquinas. Cada aluno, com o seu conjunto de máquinas virtuais, está na mesma rede, concorrendo uns com os outros num exercício comum. Este exercício pode apresentar a forma de um teste do tipo *Capture The Flag* (CTF), individual ou em grupo.

As figuras seguintes ilustram o cenário para os ensinos presencial (Figura 8) e à distância (Figura 9), o que para este exemplo configuram o mesmo tipo de exercício para ambos os modelos de ensino, uma vez que todos os alunos concorrem no ambiente virtual.

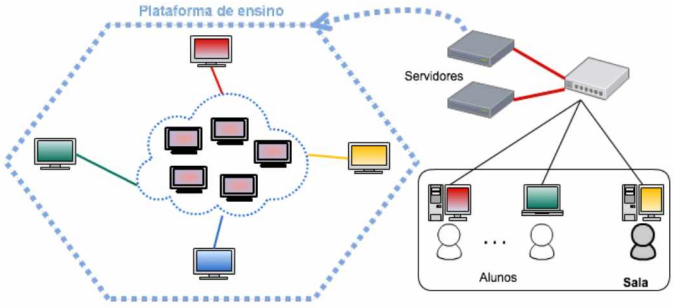


Figura 8 - Cenário 3 - regime de ensino presencial - TESTE / CTF

Estar na sala de aula ou noutro local, o importante é estar no ambiente virtual para realizar o teste ou o desafio.

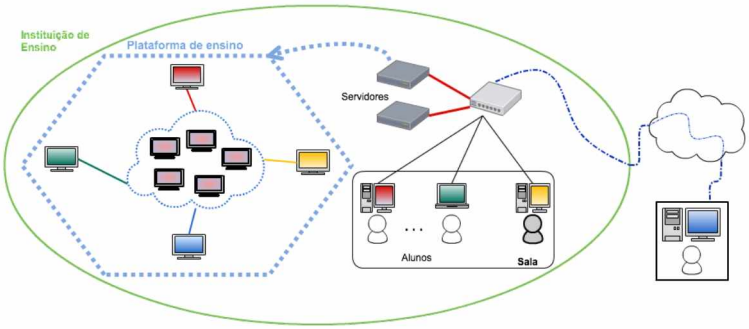


Figura 9 - Cenário 3 - regime de ensino à distância - TESTE / CTF

Procura-se, em termos de ensino, que os alunos ganhem competências técnicas na aplicação dos conhecimentos adquiridos ao nível do *hacking* e utilização das ferramentas trabalhadas ao longo das aulas. Estas são aplicadas em desafios "mãos na massa" como o que foi aqui ilustrado.

4.3 Realização de trabalhos

Num ambiente de aprendizagem maioritariamente prático, os trabalhos são um dos elementos fundamentais para o sucesso dos alunos, para a sua prática, e claro, para uma aprendizagem adequada. Assim, as aulas práticas, em regime presencial, à distância ou misto, têm nesta componente um ponto importante, para o aluno, e para o professor.

Para o aluno, por ter a possibilidade de implementar, verificar, testar e aprender num ambiente controlado, uma situação do dia-a-dia e até mesmo um cenário que pode ser uma réplica do mundo real.

Para o professor, pode mostrar, ensinar, avaliar e melhorar as competências dos seus alunos com recurso a situações práticas reais ou não, mas sempre em ambiente controlado, por um lado para que não se cometam irregularidades legais, por outro lado para que os seus alunos possam estar melhor preparados para o mercado e mundo reais.

No regime de ensino presencial e misto torna-se fácil identificar cada aluno aquando da realização dos trabalhos. O professor acompanha e conhece os alunos, e, garante a sua identidade. Desta forma, cada trabalho é do aluno em causa e o professor conhece-o.

No regime de ensino à distância, esta mesma situação de identidade, torna-se mais difícil. O aluno não está fisicamente na sala, está ligado ao ambiente de ensino e a realizar nele as suas tarefas – então como garantir que o aluno é quem diz ser?

Para minimizar esta fragilidade, propõem-se algumas soluções, para as aulas e laboratórios, que passam por:

i) atribuição e uso de um equipamento de hardware específico, pré-configurado, que se liga, de forma segura e transparente, à rede da Instituição de Ensino, o qual permite verificar o seu utilizador formal;
ii) configuração do computador do aluno para que este aceda à plataforma de ensino de técnicas de *hacking*.

Nos casos i) e ii) para as aulas e laboratórios, são necessárias configurações específicas para acesso à rede e ao ambiente da plataforma de ensino de técnicas de *hacking*. Estas configurações passam por duas etapas:

1. Acesso à rede da Instituição de Ensino (local ou remota);
2. Acesso ao ambiente da plataforma para o ensino de técnicas de *hacking*.

No caso da etapa 1. localmente, em sala ou laboratório dedicado para o efeito com acesso à rede da plataforma de ensino de técnicas de *hacking* e usando a infraestrutura de rede existente, conectam-se usando os computadores da sala ou os pessoais. Para o acesso remoto usando o equipamento de hardware referido anteriormente, que se conecta, via VPN, à rede da Instituição de Ensino. Este equipamento adiciona um reforço nas medidas de segurança, face à utilização de uma ferramenta de software para acesso VPN, uma vez que será mais difícil de "contornar" o hardware do que o software.

Uma vez na rede, passa-se à etapa 2. para aulas e laboratórios, usando o computador do aluno, este precisa ser configurado para aceder à plataforma de ensino de técnicas de *hacking* (ver Apêndice 1). Os computadores da sala já se encontrarão configurados, caso não aconteça, procede-se da mesma forma que nos computadores dos alunos.

Após estas etapas, cada aluno acede ao seu ambiente virtual, onde se encontram as máquinas virtuais para realização das aulas, laboratório, ensaios e desafios, usando os seus dados de utilizador da plataforma de ensino de técnicas de *hacking*.

4.4 Realização de elementos de avaliação

Não se pode perder de vista o facto da plataforma de ensino de técnicas de *hacking*, ser isso mesmo – uma plataforma de e para o ensino. Assim, podem-se considerar diversos e diferentes elementos para proceder à avaliação dos alunos. Estes elementos de avaliação passam pelos referidos anteriormente, numa perspetiva de avaliação contínua dos alunos, e, pela avaliação e certificação formal dos alunos nos regimes de ensino presencial, à distância ou misto.

A identificação dos alunos, conforme referido no ponto anterior, no regime de ensino presencial e misto é facilitada pelo facto de todos estarem fisicamente em sala. O professor acompanha e conhece cada aluno, e, garante a sua identidade. Desta forma, cada trabalho avaliado é do aluno em causa e o professor conhece-o.

No regime de ensino à distância, procede-se como descrito no ponto anterior, acrescentando que existe, nos serviços, a documentação do aluno aquando da sua

inscrição, que contribui para identificar o aluno. Assim, e para a avaliação e certificação formal, as propostas passam por:

i) os alunos realizarem estas provas, teóricas e/ou práticas, fisicamente na Instituição de Ensino;
ii) a Instituição de Ensino estabelecer uma rede de parceiros idóneos, para a avaliação formal, distribuída no território de abrangência dos seus alunos;
iii) uso de um CR-ROM e/ou USB Pen Drive com o sistema operativo de *boot* configurado para aceder à plataforma de ensino de técnicas de *hacking*.

Nos casos i), ii) e iii) para a avaliação e certificação formal, à semelhança das aulas e laboratórios, são necessárias configurações específicas para acesso à rede e ao ambiente da plataforma de ensino de técnicas de *hacking*, para a realização dos testes. Estas configurações passam pelas mesmas duas etapas já referidas:

1. Acesso à rede da Instituição de Ensino (local ou remota);
2. Acesso ao ambiente da plataforma para o ensino de técnicas de *hacking*.

No caso da etapa 1. para acesso local à rede, em sala ou laboratório dedicado para o efeito com acesso à rede da plataforma de ensino de técnicas de *hacking* e usando computadores existentes na sala. Para o acesso remoto usando o equipamento de *hardware* referido, que se conecta, via VPN, à rede da Instituição de Ensino.

Configurada a rede, passa-se à etapa 2., para a avaliação e certificação formal, o acesso pode fazer-se com recurso a uma imagem de *boot* em CD-ROM e/ou em USB *Pen Drive*. Este sistema está pré-configurado com todas as ferramentas necessárias para que os alunos tenham as mesmas condições de realização da avaliação e certificação formal.

Da mesma forma e após estas etapas, cada aluno acede ao seu ambiente virtual, onde se encontram as máquinas virtuais para realização da avaliação e certificação, usando os seus dados de utilizador da plataforma de ensino de técnicas de *hacking*.

IMPLEMENTAÇÃO DA PLATAFORMA

Neste capítulo serão abordados os assuntos relacionados com a implementação, arquitetura e parametrização, atividades e automatismos de gestão da plataforma de ensino SCENARIOS.

5 Implementação da plataforma

As plataformas comerciais das empresas de certificação apresentam-se fechadas e direcionadas para os exames das certificações que comercializam.

Para que esta plataforma de ensino possa ser criada é preciso idealizar e analisar a estrutura de suporte a essa implementação, uma vez que com esses mesmos objetivos e características, não existem soluções implementadas que se possam usar.

A plataforma de ensino de técnicas de *hacking*, como defendido ao longo deste trabalho, vem integrar a estrutura de suporte ao processo de ensino e aprendizagem que se encontra em utilização generalizada no ensino superior, nomeadamente o *moodle* [13] enquanto plataforma de apoio e distribuição de conteúdos em regime controlado, para as diferentes disciplinas.

O trabalho agora apresentado propõe implementar uma plataforma para o ensino de técnicas de *hacking* com recurso a tecnologia *open source* e de baixo custo, com enfoque na prática e nas aprendizagens, a que passaremos a designar por plataforma de ensino SCENARIOS, plataforma SCENARIOS ou apenas SCENARIOS.

Uma das necessidades fundamentais é a virtualização de equipamentos e sistemas com conectividade de rede, outra, é a necessidade de diferentes perfis de utilizador, para que cada aluno e professor possam atingir os objetivos pedagógicos que se propõem, assentes na análise das atividades a desenvolver, nas aprendizagens e modelos de ensino, processos de avaliação e na perspetiva da sua utilização prática.

Estes são os fios condutores que norteiam a implementação da solução apresentada nesta dissertação.

O ponto de partida para implementação da plataforma de ensino de técnicas de *hacking* é o software de virtualização que se optou por usar e cuja escolha foi feita no capitulo 3, o Proxmox VE. Esta iniciou-se com a instalação do sistema de suporte e gestão, seguindo as suas recomendações de *hardware* [17], e a sua configuração [26] na rede da Instituição de Ensino.

As secções seguintes deste capítulo abordam os requisitos e arquitetura de *hardware* necessários à implementação da plataforma de ensino SCENARIOS, parametrização de software para a sua configuração e utilização, atividades ao nível da gestão e automatização de procedimentos.

5.1 Arquitetura de hardware

A plataforma de ensino SCENARIOS, tem por base um servidor dedicado com *hardware* para servidor, em especial: memória RAM e espaço de armazenamento, seguindo os requisitos do *software* escolhido para a suportar.

Para que a plataforma funcione em prol dos alunos e das suas aprendizagens, é precisa uma infraestrutura de rede que suporte os acessos ao ambiente virtual da plataforma SCENARIOS. A infraestrutura de rede contempla bastidor, ativos de rede para o *core* da topologia e cablagem dedicada.

Os cenários de arquitetura que se seguem refletem da análise de requisitos e crescimento da plataforma SCENARIOS. Olhando para um futuro próximo, no âmbito do ensino de técnicas de *hacking* e noutros cursos e formações, espera-se que a utilização real da plataforma possa surgir. É com este objetivo no horizonte que surgem os diferentes cenários de arquitetura analisando um conjunto de possibilidades e dimensões de utilização.

Ficam algumas notas e considerações sobre os cenários de arquitetura apresentados:

- os servidores apresentados estão em *cluster* com balanceamento de carga de processamento e memória, podendo ser escalados em número, caso as necessidades aumentem;
- as ligações de rede dos servidores são a 10 GBit em portas SFP/SFP+, para garantir acessos de rede rápidos quando escalamos a solução;
- a quantidade de máquinas para alunos podem estar fisicamente separadas, assumindo o espaço de várias salas, ou apenas uma de grande dimensão;
- os acessos VPN terão equipamento dedicado e pré-configurado para aceder à rede da Instituição de Ensino.

5.1.1 Cenário de arquitetura – sala / laboratório

Este cenário de arquitetura, ilustrado na Figura 10, é o que tem a implementação mais simplificada em termos de infraestrutura de rede.

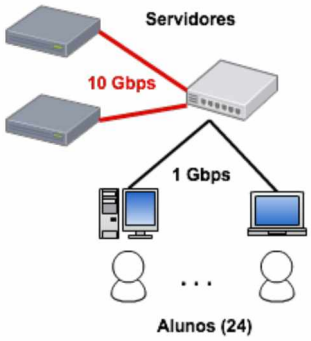


Figura 10 - Cenário de arquitetura para sala ou laboratório

Apresenta uma infraestrutura de rede com *switch* de core de 24 portas a GBit e 2 portas SFP/SFP+ a 10 GBit, cablagem UTP Cat. 6. Esta infraestrutura vai permitir comunicações com os clientes a 1 Gbps, e, com os servidores a 10 Gbps.

Podemos ter uma sala em utilização com o máximo de 24 alunos a aceder à plataforma SCENARIOS, em regime de ensino presencial, usando, ou não, os seus computadores pessoais.

5.1.2 Cenário de arquitetura – sala grande

Nesta solução, representada na Figura 11, podemos considerar duas salas separadas, uma sala grande ou auditório, com um máximo de 48 acessos para alunos. Os acessos aos servidores, mesmo entre salas, continua a estar nos 10 Gbps e para os clientes 1 Gbps.

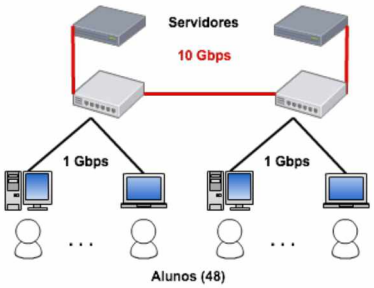


Figura 11 - Cenário de arquitetura para auditório ou duas salas/laboratórios

Por outro lado, podemos colocar uma servidor em cada *switch* para repartir a carga de utilização na rede de forma a que não se comprometa a largura de banda e os tempos de espera por parte dos clientes.

5.1.3 Cenário de arquitetura - crescimento

Este cenário permite uma solução crescente, quer em número de servidores, quer em número de salas, isto é, criamos uma estrutura de core para os servidores, com *switching* de alto débito, e num nível mais abaixo podemos adicionar salas de aula aumentando a estrutura de *switching*, como podemos observar na Figura 12.

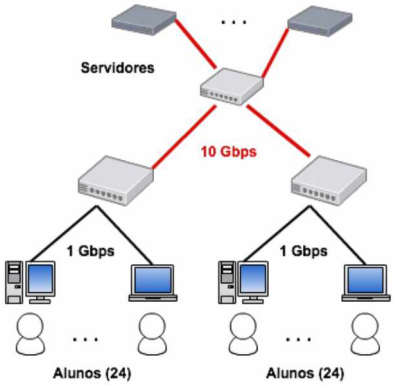


Figura 12 - Cenário de arquitetura escalável em servidores, clientes ou espaços

O crescimento da infraestrutura deve ser considerado de forma sustentada e que não comprometa a qualidade dos serviços que se pretendem implementar.

5.1.4 Cenário de arquitetura – à distância

No cenário de arquitetura ilustrado pela Figura 13, os alunos em regime de ensino à distância, ligam-se à rede da Instituição de Ensino via VPN com *hardware* específico e pré-configurado.

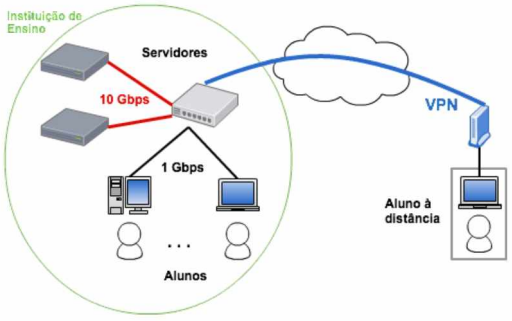


Figura 13 - Cenário de arquitetura para ensino à distância

A cada aluno é fornecido, aquando da inscrição/matrícula, um *hardware* específico e pré-configurado para acesso seguro, via VPN, à rede da plataforma SCENARIOS. Esta opção está relacionada com a segurança e acessos seguros à plataforma, segurança da rede de suporte ao ensino à distância e a garantir que o ambiente de trabalho da plataforma SCENARIOS é controlado e com acessos conhecidos.

Não nos podemos esquecer que algumas das atividades e tarefas relacionadas com o ensino de técnicas de *hacking*, feitas fora de um ambiente controlado, podem incorrer em crime informático.

Podem ainda haver alunos em regime presencial a aceder à infraestrutura de rede da sala de aula em simultâneo.

5.2 Parametrização de software

Após a instalação e configuração do servidor, procedeu-se à preparação da estrutura de *software* de suporte à plataforma. Foram consideradas como áreas de trabalho:

- Servidor;
- Utilizadores;
- Máquinas virtuais e *templates*.

5.2.1 Servidor

De acordo com as recomendações [17], e em especial em termos de processamento, memória e armazenamento, como ilustra a Figura 14, procedeu-se à instalação do sistema de virtualização da plataforma SCENARIOS, na rede da Instituição de Ensino.

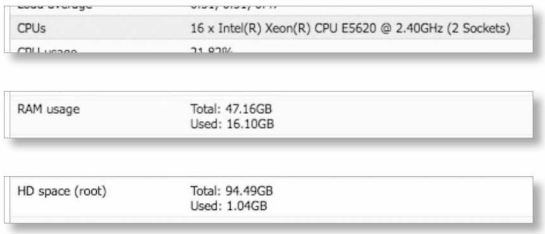


Figura 14 - Algumas características do servidor

No que respeita à rede, como se pode observar na Figura 15, determinou-se que a plataforma de ensino teria o IP `192.168.69.150/24` e responderia a pedidos no porto `8006`. Para se aceder ao ambiente gráfico (GUI) da plataforma usamos o URL `https://192.168.69.150:8006`.

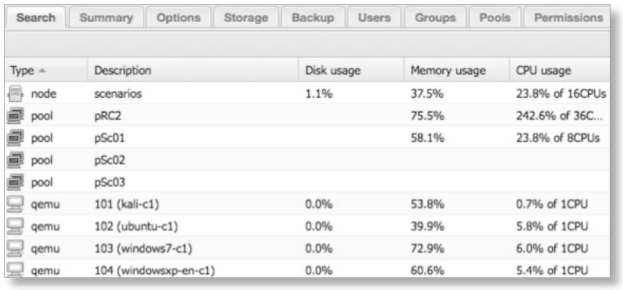
th1	Network Device	Yes	Yes				
mbr0	Linux Bridge	Yes	Yes	eth0	192.168.69.150	255.255.255.0	192.168.69.254
mbr1	Linux Bridge	Yes	Yes	eth1	192.168.0.1	255.255.255.0	

Figura 15 - Configurações de rede

Foram atribuídas às duas placas de rede do servidor, `eth0` e `eth1`, as VLAN `vmbr0` e `vmbr1` respetivamente, sendo que a rede `vmbr0` tem configurado acesso à internet através do *gateway* `192.168.69.254`.

Para ilustrar diferentes áreas de informação e configuração do servidor, apresentam-se algumas figuras. Nestas figuras podem ser observadas as opções e escolhas feitas para a plataforma SCENARIOS.

A Figura 16 ilustra o conjunto de todos os recursos já configurados na plataforma SCENARIOS. Estes podem ser pesquisados, por exemplo para localizar uma VM.

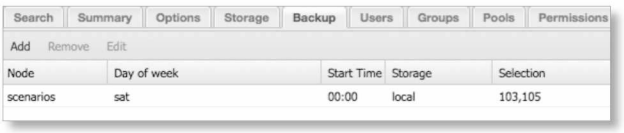


Search | Summary | Options | Storage | Backup | Users | Groups | Pools | Permissions

Type	Description	Disk usage	Memory usage	CPU usage
node	scenarios	1.1%	37.5%	23.8% of 16CPUs
pool	pRC2		75.5%	242.6% of 36C...
pool	pSc01		58.1%	23.8% of 8CPUs
pool	pSc02			
pool	pSc03			
qemu	101 (kali-c1)	0.0%	53.8%	0.7% of 1CPU
qemu	102 (ubuntu-c1)	0.0%	39.9%	5.8% of 1CPU
qemu	103 (windows7-c1)	0.0%	72.9%	6.0% of 1CPU
qemu	104 (windowsxp-en-c1)	0.0%	60.6%	5.4% of 1CPU

Figura 16 - Servidor | Geral

Na Figura 17 pode observar-se a agenda de *backups* que estão definidos e quais as VMs que estão implicadas nessa tarefa. Podem ser adicionadas e calendarizadas mais tarefas de *backup*, usando o botão **Add** [27].



Search | Summary | Options | Storage | Backup | Users | Groups | Pools | Permissions

Add | Remove | Edit

Node	Day of week	Start Time	Storage	Selection
scenarios	sat	00:00	local	103,105

Figura 17 - Servidor | *Backup*

Os recursos do servidor podem ser agrupados para uma gestão mais agilizada, a Figura 18, mostra exemplos de conjuntos de **Pools**, por exemplo, `pSc02`, contem o conjunto de VMs e armazenamento, para o cenário de ensino de técnicas de *hacking* 02.

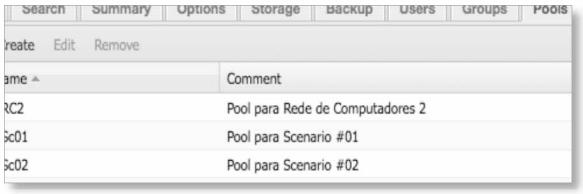


Figura 18 - Servidor | Pools

A Figura 19, mostra a lista de papéis / perfis (*Roles*) de utilizador, que estão analisados no 5.2.2 Utilizadores, deste trabalho, no entanto são de realçar o `PVEAdmin`, `PVEPoolAdmin`, `PVETemplateUser`, `PVEUserAdmin`, `PVEVMAdmin` e `PVEVMUser`.

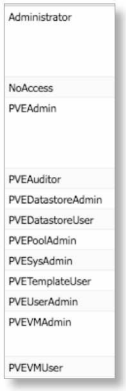


Figura 19 - Servidor | Roles

Em resumo foram preparadas, ao nível do servidor, as tarefas de armazenamento de dados, *pool* de recursos, estrutura de utilizadores, privilégios e grupos de trabalho, para as máquinas virtuais que suportam os cenários de ensino de técnicas de *hacking*.

5.2.2 Utilizadores

Os utilizadores propostos neste trabalho são fruto da análise da implementação efetuada e dos ensaios e experiências em sala de aula que foram realizados.

Cada utilizador tem um nome e palavra-passe para aceder à sua área da plataforma, e nela efetuar as tarefas que lhe competem. Desta forma definiram-se os seguintes tipos de utilizador:

- Alunos ou formandos – este tipo de utilizador é atribuído a cada aluno na plataforma SCENARIOS;

- Professores ou formadores – este role é atribuído aos professores na plataforma de ensino;

- Suporte e Apoio – este papel é atribuído aos utilizadores da equipa de suporte e apoio à plataforma SCENARIOS e aos seus utilizadores;

- Administrador – este papel é atribuído aos utilizadores da equipa de gestão e administração do servidor e da plataforma SCENARIOS.

É de salientar que para os papéis de Suporte, Apoio e Administrador, pode ser considerada a mesma pessoa, em função da dimensão da plataforma de ensino. No caso desta estar em utilização na Instituição de Ensino, com alunos presenciais e à distância e com um volume de VMs considerável, devem estes papéis passar a estar em diferentes pessoas e integrados numa equipa de trabalho multidisciplinar, para que também os aspetos pedagógicos sejam assegurados, e consequentemente as boas aprendizagens dos alunos.

A cada um foi atribuído um ou vários grupos, papéis e respetivas permissões (*Roles*), e VM(s). A Figura 20, mostra parte da lista de utilizadores, juntamente com algumas informações de cada conta de utilizador, nomeadamente, o nome, se está ou não ativa e quando expira.

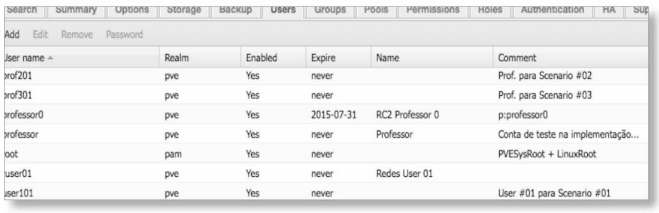


Figura 20 – Dados sobre utilizadores - *Users*

A juntar às características dos utilizadores, tal como referido anteriormente, estes podem estar integrados em grupos de trabalho. Estes grupos permitem que a gestão de permissões e perfis possam afetar todos os membros do grupo, por exemplo, para

o grupo `gSc01`, representado na Figura 21, podem ser ajustadas as permissões para os seus membros e para as máquinas virtuais que lhe pertençam.

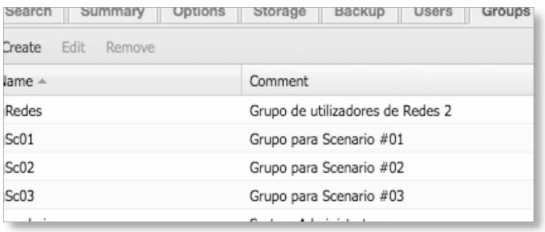


Figura 21 – Utilizadores e VMs - *Groups*

Desta forma, se o cenário de ensino for do tipo *Capture The Flag* (CTF), e para que uma nova VM possa ser acedida pelos alunos, basta adicioná-la ao grupo desse cenário para que todos os seus membros lhe tenham acesso. Este acesso pode, por exemplo, ser à consola da máquina virtual.

As permissões de cada utilizador sobre o conjunto de recursos que lhe está afeto, depende do perfil de utilizador que lhe for atribuído.

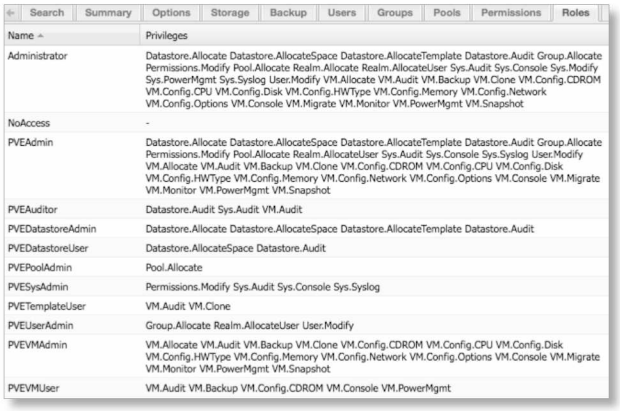


Figura 22 – Perfis e Permissões de Utilizador - *Roles*

Na Figura 22, podemos observar os diferentes perfis que podem ser atribuídos aos utilizadores e as respetivas permissões associadas.

5.2.2.1 Alunos

A plataforma SCENARIOS foi construída para que os alunos possam aprender técnicas de hacking num ambiente controlado e que permita testar, experimentar, consolidar e aprender novos conhecimentos.

Os perfis mais comuns atribuídos ao aluno são o de `PVEVMAdmin` e de `PVEVMUser`, uma vez que, cada aluno precisa de ter administração sobre a sua VM, e pode, por

exemplo, visualizar o ecrã da máquina virtual (`VM.Console`) do professor, precisando para tal de lhe aceder com privilégios limitados, no perfil de `PVEVMUser`, tal como pode ser observado na Figura 23.

Figura 23 - Perfis e Permissões do Aluno

5.2.2.2 Professores

O papel do Professor na plataforma de ensino SCENARIOS, é o de acompanhar a evolução dos alunos, permitindo aprendizagens sustentadas e crescimento académico, lançar novos desafios e avaliar o desempenho de cada aluno. Em conjunto com o Suporte e Apoio e/ou SysAdmin, criar e desenhar os cenários que serão aplicados nas aprendizagens dos seus alunos, caracterizando os sistemas a utilizar, software, máquinas virtuais, redes e VLAN.

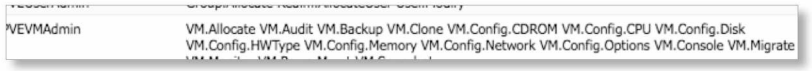


Figura 24 – Perfil e Permissões do Professor

Em termos de perfis de utilizador na grande maioria dos casos este é de `PVEVMAdmin`, seja sobre as suas VMs, ou sobre as VMs dos seus alunos, com as características que se observam na Figura 24.

Com vista ao melhoramento das aprendizagens e práticas em sala de aula, presencial ou virtual, o perfil de cada professor pode ser ajustado face às suas necessidades e conhecimentos específicos.

5.2.2.3 Suporte e Apoio

Este papel tem duas vertentes, suporte e apoio para os alunos e professores na configuração dos seus computadores e equipamentos para acesso à rede e com ajustes nas VMs e áreas de trabalho online.

No que respeita aos perfis de utilizador, e de acordo com as tarefas definidas, estes podem incluir: `PVEAuditor`, `PVEDatastoreUser`, `PVEPoolAdmin`, `PVETemplateUser`, `PVEUserAdmin` e `PVEVMAdmin`. As tarefas de cada um podem ser observadas na Figura 25.

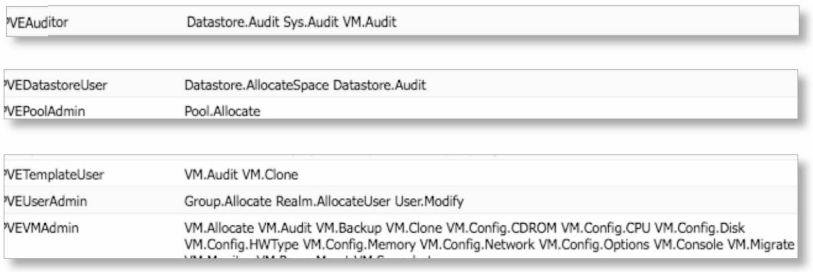


Figura 25 - Perfis e Permissões do Suporte e Apoio

5.2.2.4 Adminsitrador

O SysAdmin, nos perfis de `Administrator` (para o servidor) e `PVEAdmin` (para a plataforma de ensino) é responsável pelo sistema que suporta a plataforma, configurações, atualizações, *backups*, gestão da rede de suporte aos servidores, gestão de recursos e utilizadores, atribuição das máquinas virtuais a cada utilizador, grupo, ou *pool* de recursos. Pode, ainda, integrar, substituir, apoiar e formar a equipa de Suporte e Apoio nas suas tarefas.

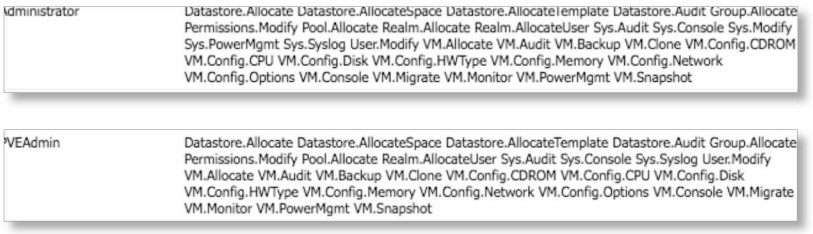


Figura 26 - Perfil do Adminsitrador

5.2.3 Máquinas virtuais e templates

Num primeira fase foram criadas e instaladas as máquinas virtuais com os Sistemas Operativos (SO) que, à data, são necessários para a criação dos cenários de ensino de técnicas de *hacking*, nomeadamente:

- Kali Linux;
- Microsoft Windows XP;
- Microsoft Windows 7;
- Ubuntu Linux Desktop e Server;
- Metasploitable 2.

As características de *hardware* de cada VM são definidas de acordo com as indicações do professor, no entanto, e para que possa haver algum procedimento base, cada VM está caracterizada, em termos de *hardware* conforme apresenta a Figura 27.

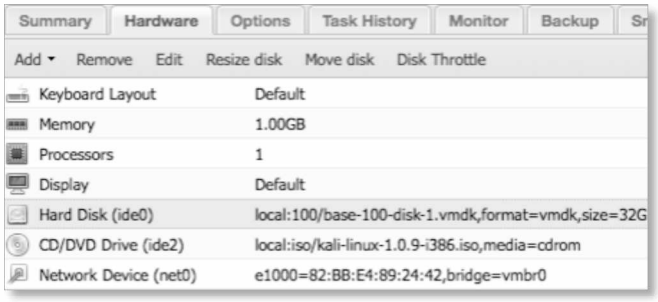


Figura 27 - Características de *hardware* base das VMs

Podem ser adicionados componentes de *hardware* à máquina virtual, usando o botão **Add**, bem como ajustados os parâmetros dos existentes, recorrendo à barra de botões (Figura 27).

Uma vez feita a sua instalação base, cada máquina virtual foi convertida para o respetivo *Template* (Figura 28).

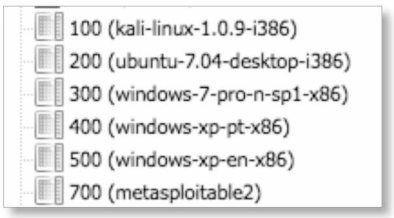


Figura 28 - Templates paracriação de VMs

Esta operação vai permitir a adição de VMs a partir dos *templates* criados, tornando assim o processo de adicionar máquinas virtuais bastante mais rápido, simplificado e automático.

As fases seguintes da configuração das máquinas virtuais passam pela sua associação aos utilizadores e/ou grupos (Figura 29), *Pool* de recursos (caso seja necessário), VLAN e configurações de rede do cenário definido pelo professor.

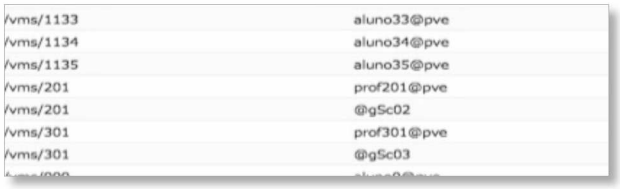


Figura 29 – Associação das VMs aos Utilizadores/ Grupos

Pode ser preciso, de acordo com as indicações do professor, para a implementação do cenário de ensino, proceder a atualizações ao sistema. Estas atualizações processam-se com a VM em execução e no respetivo sistema.

Espera-se, com o crescimento de utilização da plataforma, que novos sistemas sejam carregados para que se possam criar mais e novos cenários de ensino.

5.3 Atividades de gestão

As atividades de gestão fazem parte dos alicerces e fundições da plataforma SCENARIOS. Algumas dessas atividades já foram mencionadas e explicadas nos pontos anteriores. Passam pela criação de templates e alguns *scripts* de automatização de tarefas, e, ainda do apoio aos utilizadores, em especial aos professores na criação dos cenários de trabalho para as suas aulas. Estas últimas para que possamos ter o nível de sucesso nas aprendizagens dos alunos, bem como, dos acessos à plataforma, avaliações e certificações, rigor e seriedade na recolha de todos os elementos de avaliação dos alunos, estejam eles em sala de aula ou remotamente via VPN.

É na gestão da plataforma SCENARIOS que o perfil de Suporte e Apoio tem as suas tarefas fundamentais, quer para com os professores e alunos, quer para com a plataforma.

As tarefas efetuadas pela equipa de apoio e suporte são as atividades de gestão propriamente ditas, isto é, e tal como mencionado anteriormente, configuração dos computadores e equipamentos, dos professores e alunos, para acesso à rede e à plataforma de ensino SCENARIOS, e com ajustes nas máquinas virtuais, de acordo com os cenários a implementar e áreas de trabalho online.

5.4 Automatização de procedimentos

Os procedimentos automatizados tendem a crescer com a utilização e as necessidades dos utilizadores da plataforma. No entanto, e na fase em que nos encontramos, temos um conjunto de tarefas que podem ser feitas de forma automática, como por exemplo:

- arranque automático das VMs – com o arranque do servidor da plataforma podem ser indicadas as máquinas virtuais que devem iniciar;
- criação de *templates* de instalação de máquinas virtuais com diferentes sistemas operativos, até mesmo em diferentes fases de atualização dos sistemas;
- utilizadores e grupos de trabalho– adicionar, alterar e gerir as contas de utilizadores é um trabalho constante. Podem ser criados alguns scripts que agilizem as tarefas repetitivas e de controlo de utilizadores e grupos de trabalho;
- perfis e permissões – os utilizadores e máquinas virtuais, podem, pontualmente ou de forma definitiva, precisarem de ser ajustados e/ou alterados. A sua gestão pode igualmente ser agilizada pela criação de alguns scripts de automação desta gestão;
- *pool* de recursos – o mesmo se verifica ao nível da gestão e manutenção dos recursos;
- paragem de uma ou várias VMs – a paragem (stop) de uma ou várias máquinas virtuais, ou mesmo do conjunto de um cenário de ensino, é outro exemplo.

Alguns dos procedimentos referidos nesta fase não são totalmente automatizados, sendo necessária a intervenção da equipa de suporte e apoio. Reforça-se a necessidade de utilização efetiva para identificar e clarificar estes e outros processos e procedimentos a automatizar.

Para aqueles em que seja possível a total automação, e para os que surjam e não tenham sido contemplados neste trabalho, remete-se a sua implementação para trabalhos futuros.

ABORDAGEM AO ENSINO DE TÉCNICAS DE HACKING

Neste capítulo serão abordados os assuntos relacionados com as taxonomias e classificação de ataques, conceitos, instituições envolvidas neste processo e protótipo de módulo de ensino.

6 Abordagem ao ensino de técnicas de hacking

Nos últimos anos os ataques têm vindo a aumentar, bem como a sua sofisticação, isto é, aumentaram de forma significativa pondo em risco os dados, utilizadores de sistemas informáticos e redes de computadores e comunicações. Torna-se cada vez mais importante e necessário olhar para cada ataque de uma forma detalhada de maneira que se possa "combater" usando mecanismos efetivos e consistentes.

Entre outros, existem alguns conceitos que são importantes pelo enquadramento dos termos e pela sua importância no processo de ensino. Seguindo esta orientação, ficam alguns dos conceitos base:

Ataque – um ataque corresponde ao uso de um ou vários *exploits* para tirar vantagem/partido de uma falha/debilidade/fragilidade com intenção de atingir negativamente um sistema ou rede informática.

Atacante – é aquele que efetua o ataque, podendo ser o sistema que efetua o ataque.

Ameaça – é um ataque, potencialmente de sucesso, envolvendo um adversário que utilizando técnicas e recursos específicos para tirar proveito dos pontos fracos/falhas/debilidades/fragilidades de um sistema ou organização alvo, com o objetivo de alcançar um impacto negativo sobre o alvo.

Vulnerabilidade – é uma falha/debilidade/fragilidade que pode ser usada de forma não desejada. Tipicamente corresponde à violação de uma medida de segurança de um sistema ou rede informática tendo como resultado um impacto negativo no referido sistema ou rede. Podemos considerar que todas as vulnerabilidades envolvem falhas/debilidades/fragilidades, mas, nem todas as falhas/debilidades/fragilidades são vulnerabilidades. No projeto *Common Vulnerabilities and Exposures* (CVE) [28] encontram-se os nomes e dados das vulnerabilidades relacionadas com o *software* e que são conhecidas publicamente.

Exploit – corresponde a ação de explorar/façanha e aproveitar a falha/debilidade/fragilidade(s) para afetar negativamente um sistema ou rede

informática. A existência de um *exploit* é o que transforma uma falha/debilidade/fragilidade numa vulnerabilidade.

Método de ataque – é a metodologia que classifica o ataque, podendo ser por exemplo usado o *Common Attack Pattern Enumeration and Classification* (CAPEC) [29] para a sua classificação, em conjunto, ou não, com outros tipos de classificação.

Padrão de ataque – um padrão de ataque é um mecanismo abstrato que ajuda a compreender e descrever a forma como um ataque é executado. Cada padrão determina/define o "desafio" que um atacante tem de enfrentar/executar, descreve as técnicas usadas e apresenta recomendações para a mitigação do ataque em causa. Estes padrões permitem, de forma sistemática, categorizar os ataques para que as equipas de desenvolvimento e desenho dos sistemas envolvidos possam compreender como melhorar e defendê-los. O projeto *Common Attack Pattern Enumeration and Classification* (CAPEC) [29] apresenta/promove/disponibiliza uma lista organizada e classificada dos padrões de ataque conhecidos.

Vector de ataque – indica a área sobre a qual o ataque foi efetuado. De acordo com a organização e classificação dos ataques, estes podem ser agrupados/organizados em função da sua objetividade.

Feito este enquadramento, as secções seguintes deste capítulo abordam as taxonomias e classificação de ataques, instituições envolvidas neste processo e protótipo de módulo de ensino.

6.1 Instituições e organizações relevantes

A identificação, gestão e publicação de taxonomias, classificação e vulnerabilidades envolve um conjunto de instituições e empresas à escala global. Esta situação é incontornável face à realidade de que as fronteiras físicas não existem no mundo virtual e todos estes cenários são globais.

Por outro lado é necessária uma colaboração institucional e empresarial, também estas à escala global, dado que muitas das envolvidas têm dimensão global operando em diferentes países e continentes.

ENISA - European Union Agency for Network and Information Security

A agência europeia para a segurança das redes e da informação é um organismo da União Europeia (UE), criada em 2004 pela *EU Regulation No 460/2004* [30] e está operacional desde setembro de 2005 em Heraklion, Grécia. O objetivo da ENISA é melhorar a rede e segurança da informação na União Europeia. A agência tem de contribuir para o desenvolvimento de uma cultura de rede e segurança da informação em benefício dos cidadãos, dos consumidores, das empresas e organizações do setor público da União Europeia e, consequentemente, contribuirá para o bom funcionamento do mercado interno da UE. A ENISA assiste a Comissão, os Estados-Membros e, consequentemente, a comunidade empresarial no cumprimento dos requisitos de rede e segurança da informação, incluindo a legislação presente e futura da UE. Em última análise, a ENISA, esforça-se para servir como um centro de conhecimento, tanto para os Estados-Membros e as instituições da UE a procurar aconselhamento sobre questões relacionadas à rede e segurança da informação [31].

NIST – National Institute of Standards and Techonology

O National Institute of Standards and Techonology, é uma agência governamental não-regulatória da administração de tecnologia do Departamento de Comércio dos Estados Unidos. Tem como objetivos promover a inovação e a competitividade industrial dos Estados Unidos da América através do avanço da ciência de medição, padrões e tecnologia de forma a aumentar a segurança económica e melhorar a qualidade de vida [32].

CERTs – Computer Emergency Response Team

Estas equipas são constituídas por grupos de pessoas especialistas em resposta a incidentes de segurança. Podem ser conhecidos também por *Computer Security Incident Response Team* (CSIRT). O seu nome, CERT, foi inicialmente utilizado na Universidade de Carnegie Mellon, no centro coordenador do CERT (CERT-CC) [33]. Este nome e siglas acabaram por ser usados por outros centros que foram surgindo a nível global.

No caso de Portugal, o cert.pt, é um serviço do Centro Nacional de Cibersegurança (CNCS) [34]. À semelhança dos CERT de outros países, o CERT.PT, tem como principal missão contribuir para que Portugal use o ciberespaço de uma forma livre, confiável e segura, através da melhoria contínua da cibersegurança nacional e da cooperação internacional [35].

MITRE Corporation

É uma organização sem fins lucrativos que trabalha na área da pesquisa e desenvolvimento sendo financiada pelo governo americano [36]. É responsável, entre outras, pela gestão e implementação do *Common Attack Pattern Enumeration and Classification* (CAPEC) [29], *Common Weakness Enumeration* (CWE) [37], *Common Vulnerabilities and Exposures* (CVE) [28]. Estes mecanismos de classificação de ataques são amplamente usados por um grande, e crescente, número de instituições e empresas à escala global.

Industria de *Hardware* e *Software*

A industria de hardware e de software são uma das componentes que contribui para a segurança e cibersegurança da informação. Podem-se considerar igualmente as responsabilidades que a mesma indústria tem para com os ataques à segurança e cibersegurança, isto é, na criação e desenvolvimento de produtos que sejam seguros, quer de *hardware* quer de *software*.

Cada empresa, que desenvolve produtos de *hardware* e/ou de *software*, tem o dever de registar, informar e corrigir as falhas nos seus produtos, sejam encontradas pelas próprias empresas ou por terceiros que as comuniquem, às entidades competentes, bem como, aos seus fabricantes. Foram identificadas, nos pontos anteriores, algumas das entidades envolvidas neste processo.

As vulnerabilidades que permitem implementar as técnicas de *hacking*, cuja exploração permite o acesso aos sistemas e dados, estão intimamente relacionadas com a indústria tecnológica do *hardware* e *software*.

6.2 Taxonomias e classificação de ataque

Neste âmbito, as taxonomias e classificação dos ataques são muito úteis uma vez que nos permitem organizar, compreender, classificar e quantificar os ataques no seu todo. Hoje em dia fala-se muito nos ataques, no entanto a linguagem usada para os caracterizar nem sempre é de conteúdo fácil e claro, ou mesmo consistente. Por exemplo: para uma mesma ocorrência do tipo vírus, uns podem considerá-la como *worm* e outros não, causando uma abordagem distinta ao mesmo problema.

A necessidade de uma linguagem consistente e comum para classificar um ataque pode ser fornecida por uma taxonomia consistente. Esta consistência irá permitir que no caso de novos ataques se possa usar o conhecimento dos anteriores para lidar com o novo ataque.

Existem diferentes intervenientes que beneficiam do uso de uma taxonomia desta natureza, como por exemplo, os *Computer Emergency Response Team* (CERT). Todos eles ganham com a utilização de uma linguagem comum, evitando confusões na classificação dos ataques e "falando" a mesma língua.

Em género de resumo, e na área das redes de computadores e segurança informática, existem várias taxonomias para classificação de ataques nos últimos tempos [38]:

6.2.1 Taxonomias de segurança iniciais

As duas iniciais que surgiram na área da segurança foram a *Protections Analysis Taxonomy* [39] e a *Research in Secured Operating Systems Taxonomy* [40]. Estas eram focadas nas vulnerabilidades dos sistemas em vez de nos ataques. Eram baseadas no registo de falhas de segurança e a sua classificação em classes. A sua discrepância residia no facto de haver ambiguidade entre as suas classes de classificação. Havia vulnerabilidades que eram comuns a diferentes classes, criando desta forma dificuldade na sua classificação. Apesar disso os conceitos por detrás destas taxonomias são válidos e deram origem a novas taxonomias [41,42,43].

6.2.2 Bishop's Vulnerability Taxonomy

Diferentes contribuições foram feitas neste campo por Matt Bishop. Ele apresenta [42] uma taxonomia para vulnerabilidades em sistemas UNIX, através da classificação em seis eixos de vulnerabilidades: *Nature*, *Time of introduction*, *Exploitation Domain*, *Effect Domain*, *Minimum Number* e *Source*. Bishop fez ainda um conjunto de verificações e comparações entre as abordagens anteriores [41,44], nomeadamente sobre o que torna uma taxonomia efetiva e consistente. Uma das suas conclusões/sugestões foi que uma boa taxonomia deve indicar/ajudar a decidir onde investir os recursos disponíveis.

6.2.3 Howard's Taxonomy

Usando uma abordagem ao nível dos processos, John Howard, apresenta uma taxonomia que tem em consideração fatores de motivação e objetivos [45]. Na Figura 30, podemos observar a estrutura de Howard que consiste em cinco fases: *Attackers*, *Tools*, *Access*, *Results* e *Objectives*. *Attackers* é um conjunto de tipos de pessoas que podem realizar o ataque, desde *hackers* a terroristas; *Tools*, são os meios usados pelos atacantes; *Access*, é obtido pela implementação, design/criação ou configuração de uma vulnerabilidade; *Result*, após ter ganho o acesso, os resultados podem ser diversos, por exemplo, corrupção de informação; *Objectives*, através dos resultados obtidos são atingidos os objetivos propostos.

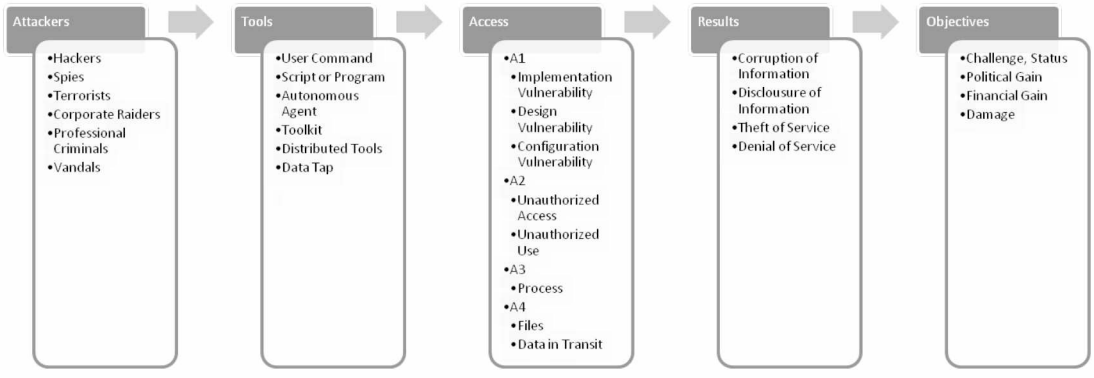


Figura 30 - Howard's Taxonomy

6.2.4 Lough's Taxonomy

Daniel Lough propôs, em 2001, uma taxonomia designada VERDICT (*Validation Expousure Randomness Deallocation Improper Conditions Taxonomy*) que se baseava

nas características do ataque [43]. A estrutura usava quatro características de ataque: *Improper Validation*; *Improper Expousure*; *Improper Randomness*; *Improper Deallocation*. A taxonomia de Lough, quando aplicada a novas tecnologias veio a verificar-se útil. Foi aplicada a 802.11 e encontrou várias vulnerabilidades. Em termos mais específicos e para a classificação do dia-a-dia a taxonomia de Lough é muito generalista.

6.3 Common Attack Pattern Enumeration and Classification

A taxonomia de ataques designada de *Common Attack Pattern Enumeration and Classification* (CAPEC) [29] foi desenvolvida pela organização MITRE [36] para o *US Department of Homeland Security*. Tem como base de trabalho o livro *Exploiting Software: How to Breack Code* [46].

O principal objetivo da lista é a criação de um conjunto/listagem de padrões de ataque usado pelos atacantes aos sistemas que sejam comprometidos. Tal como referido no site do CAPEC "*este esforço tem como objetivo documentar e publicar um catálogo de padrões de ataque conjuntamente com uma estrutura que permita a sua compreensão e classificação taxionómica*" [47].

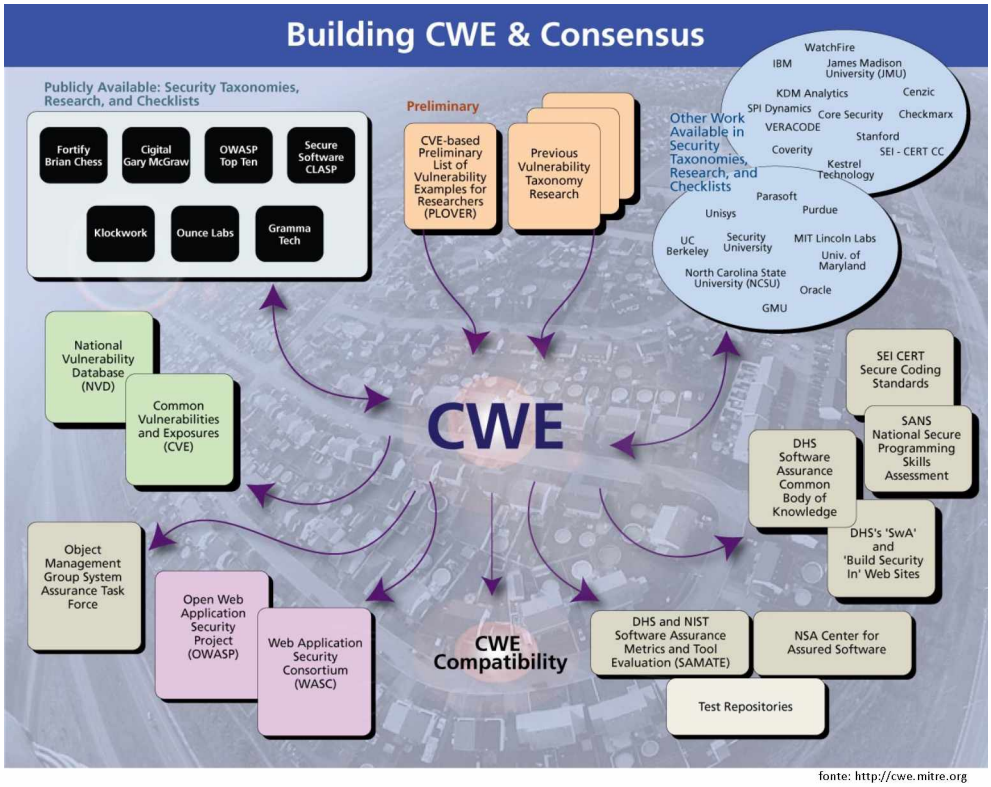
A estrutura da lista CAPEC é mantida de forma hierárquica onde a título de exemplo se apresenta o nível de topo que é constituído por onze categorias:

- *Abuse of Functionality*
- *Spoofing*
- *Probabilistic Techniques*
- *Exploration of Authentication*
- *Resource Depletion*
- *Exploitation of Privilege/Trust*
- *Injection*
- *Data Structure Attacks*
- *Data Leakage Attacks*
- *Resource Manipulation*

- *Time and State Attacks*

Para cada categoria, a lista CAPEC, contém dados sobre o padrão de ataque que incluem descrição, métodos do ataque, severidade, exemplos, relação com a lista de *Common Weakness Enumeration* (CWE) [37], *Common Vulnerabilities and Exposures* (CVE) [28] e outros campos de interesse [48].

A Figura 31, mostra as diferentes taxonomias, fontes e contributos, e entidades, instituições, empresas e fluxos de informação envolvidos neste processo de classificação, bem como o seu contributo para outras fontes e modelos de classificação existentes.



fonte: http://cwe.mitre.org

Figura 31 - Relação e contributos CWE

Corresponde a um esforço na "standarização" do registo e descrição dos padrões de ataque [29].

O registo dos padrões de ataque conhecidos de forma integrada e consistente reflete-se numa mais-valia e vantagem para toda a comunidade de utilizadores da informação.

6.4 Protótipo de módulo de ensino para Exploração de Autenticação

Nesta secção apresenta-se a criação de um protótipo de cenário baseado na taxonomia *Common Attack Pattern Enumeration and Classification* (CAPEC), no seu ramo "CAPEC-225: Exploitation of Authentication", ao nível dos "Mechanisms of Attack", para exemplo e/ou prova de conceito, sobre a utilização do modelo CAPEC [29] na implementação de currículos para o ensino de técnicas de *hacking* no âmbito desta dissertação. Os *Common Vulnerabilities Enumeration* (CVE) aprovados podem ter associados diferentes *Common Weakeness Enumeration* (CWE), em função das suas características.

Assim, e para o exemplo apresentado, o caminho a percorrer na estrutura CAPEC-225 até chegarmos ao CVE específico que queremos abordar, o CVE-2008-0166, correspondente ao ataque ao OpenSSL 0.9.8.c-1 usando força bruta para aceder às suas chaves.

Na Figura 32, podemos observar o ramo do CAPEC-225 e respetivas ramificações filhas, até ao exemplo abordado.

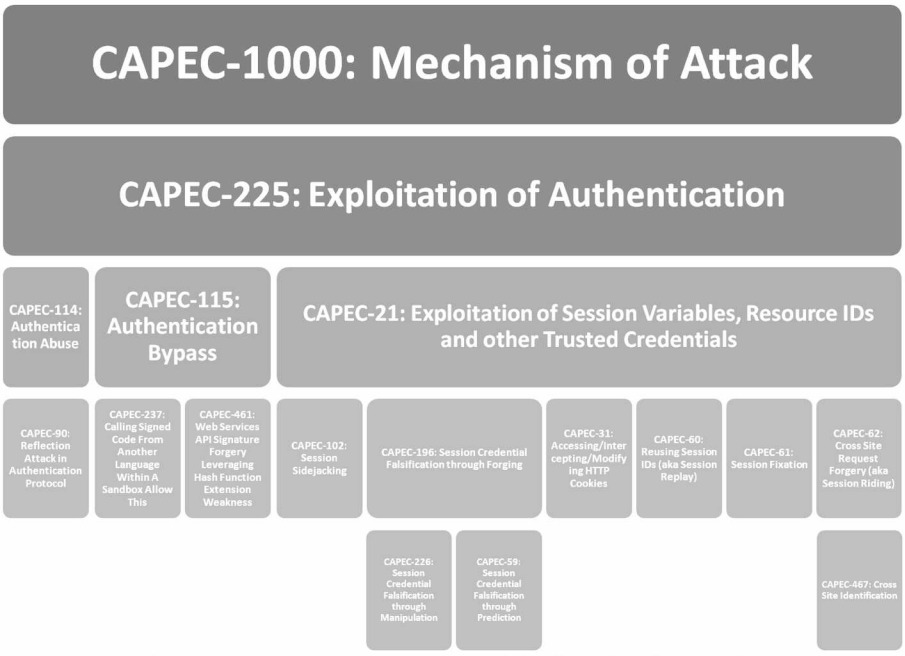


Figura 32 - Estrutura CAPEC-225: Exploitation of Authentication

Seguindo a estrutura pelo caminho CAPEC-21 --> CAPEC-196 --> CAPEC-59, como se pode observar com maior detalhe na Figura 33.

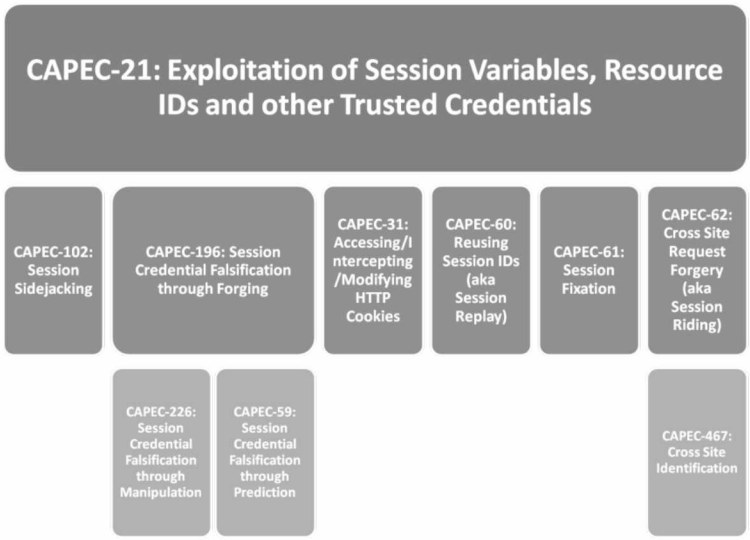
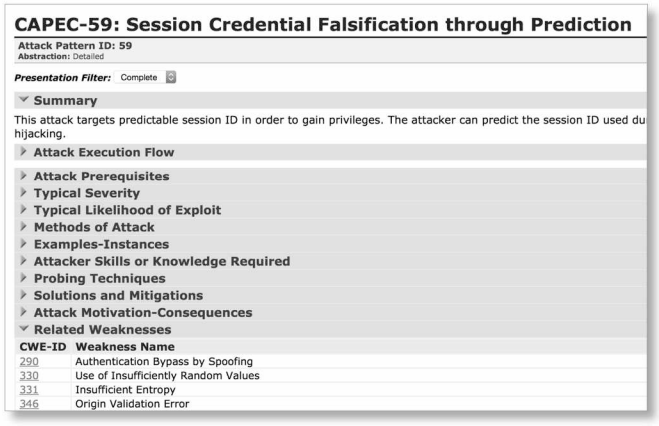


Figura 33 - Detalhe de CAPEC-21: Exploitation of Session Variables, Resource IDs and inther Trusted Credencials

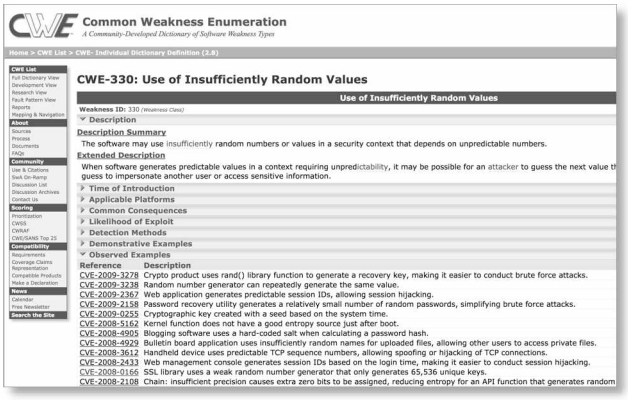
Continuando a percorrer a estrutura, chega-se ao ramo "CAPEC-59: Session Credential Falsification through Prediction", que está detalhado em [37] conforme a Figura 34.



fonte: http://cwe.mitre.org

Figura 34 - CAPEC-59: Related Weaknesses - CWE-330

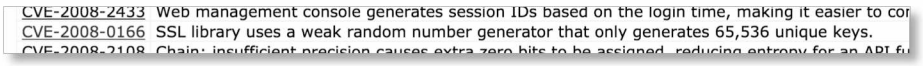
Após localizar o "CWE-330: Use of Insufficiently Random Values", e observando os seus parâmetros, em particular **Observed Examples** (Figura 35).



fonte: http://cwe.mitre.org

Figura 35 - CWE-330: Use of Insufficiently Random Values

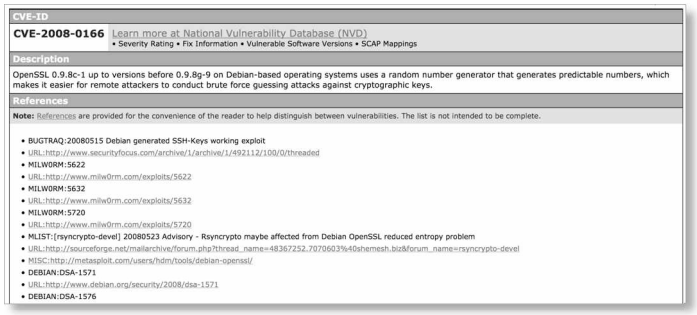
Pode-se encontrar de forma detalhada, entre outras, a vulnerabilidade a explorar, o CVE-2008-0166.



fonte: http://cve.mitre.org

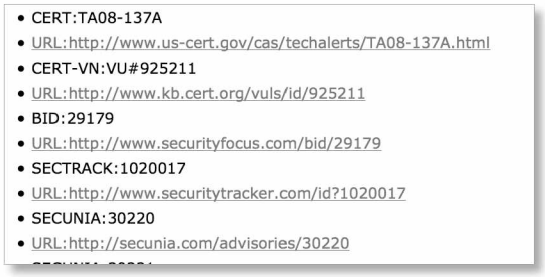
Figura 36 - Detalhe da lista CVE associados ao CWE-330

Uma vez no descritivo do CVE-2008-0166, como mostra a Figura 37, podemos aceder, via **References**, aos diferentes locais onde está detalhada a vulnerabilidade, como por exemplo, US-CERT, *securityfocus* ou *secunia* (Figura 38).



fonte: http://cve.mitre.org

Figura 37 – Detalhes do CVE-2008-0166



fonte: http://cve.mitre.org

Figura 38 - Detalhe das referências do CVE-2008-0166

Para implementar o protótipo usando o CAPEC e a sua estrutura como referência, a proposta é poder percorrê-la, até chegar ao(s) CVE(s) que detalham a vulnerabilidade a configurar/ajustar/verificar/ensinar aos alunos, conforme exemplificado anteriormente.

O protótipo tem na sua base esta estrutura uma vez que ao nível global, seja por estados, instituições e empresas, usam esta classificação como referência para catalogar e organizar os ataques, gerar classificações e quantificações dos ataques [49].

As organizações que contribuem para estas listas [50,51] em relação à sua atualização, melhoramento, utilização, reforçam a sua importância na classificação dos ataques, bem como no melhoramento dos produtos de *hardware* e *software* que são desenvolvidos, tornando-os mais seguros.

Em resumo, tomando os diferentes ramos de classificação do CAPEC, enquadramos os ataques em estudo. Percorrendo a estrutura de ramos, chega-se ao(s) CWE que clarificam o padrão de ataque em estudo. Por último, identifica-se o CVE que detalha o ataque, e, usando as diferentes fontes, pode-se reproduzir o cenário com a vulnerabilidade em estudo/ensino e usar/estudar/aprender a usar as ferramentas que permitem explorar a vulnerabilidade.

É esta abordagem ofensiva, ao nível do ensino das técnicas de *hacking*, que tem vindo a ser desenvolvida ao longo deste trabalho, e que pretende dar o seu contributo com o desenvolvimento da plataforma SCENARIOS, que suporta estes cenários e respetivas técnicas para o seu ensino.

AVALIAÇÃO

Neste capítulo serão abordados os assuntos relacionados com a avaliação da plataforma proposta, análise do seu desempenho com utilizadores reais e algumas considerações.

7 Avaliação

A proposta apresentada, plataforma de ensino SCENARIOS, pretende, de uma forma dinâmica, promover diferentes atividades letivas: aulas, laboratórios, testes e avaliações, desafios; estes podem ser individuais ou de grupo, isolados ou concorrentes, em ambiente controlado, não esquecendo os aspetos pedagógicos e do processo ensino aprendizagem, conforme descrito ao longo deste trabalho.

As diferentes configurações de utilização podem ter um ambiente de sala de aula/laboratório com um conjunto de máquinas para os alunos utilizarem, ou podem ser usados os equipamentos dos alunos para as atividades, tendo estes duas vertentes:

- acesso condicionado ao sistema do seu computador;
- acesso livre ao sistema do seu computador.

Na primeira, todos os computadores arrancam com o mesmo sistema de *boot*, enquanto que na segunda cada computador usa o seu sistema de *boot*.

As secções seguintes deste capítulo abordam a avaliação da plataforma proposta, análise do seu desempenho com utilizadores reais e algumas considerações sobre a utilização do sistema em relação aos seus aspetos pedagógicos.

7.1 Avaliação de carga

A plataforma SCENARIOS foi sujeita a alguns testes de carga e utilização com alunos, destes, registam-se dois testes de carga feitos ao sistema.

A infraestrutura de rede que foi usada depende da localização da atividade e da quantidade de equipamentos que estamos a usar, isto é, para uma atividade com um número mais reduzido de alunos, usamos a sala L11 da Escola Superior de Tecnologia e Gestão (ESTIG) com computadores de secretária. Para um número maior de utilizadores, usamos a sala S10 da ESTIG, onde foi implementada uma estrutura de rede, escalável, com ilhas de acesso para quatro utilizadores, com recurso a uma rede em estrela usando equipamento do laboratório para *switching*. Para estas localizações existe cablagem distribuída até ao bastidor onde se encontra o servidor da plataforma.

No que respeita ao sistema operativo e condições de acesso à plataforma, e para garantir que todos os alunos tenham um acesso idêntico, foi criada uma imagem, usando a distribuição de *Linux TinyCore* para que o acesso ao ambiente SCENARIOS fosse o mais transparente possível. A escolha recaiu sobre esta distribuição por esta ter um ambiente minimalista e simples, apresentar uma dimensão relativamente pequena que, depois de devidamente configurada, a imagem podia ser grava em CD-ROM e em USB *Pen Drive* de pequeno armazenamento.

Após o arranque do sistema, com as máquinas virtuais necessárias a cada utilizador em execução e devidamente configuradas com todas as ferramentas necessárias, usando uma janela de *browser* – Firefox Mozilla – estamos no ponto de *login* ao sistema de virtualização e aprendizagem SCENARIOS.

Todos os alunos se encontravam nas mesmas condições de trabalho e realização dos testes, dando-se início aos mesmos.

Em termos de análise a estes testes foram registadas e observadas a utilização, ao nível da plataforma SCENARIOS e os parâmetros: `CPU Usage`, `Memory Usage` e `Network Traffic`.

7.1.1 Teste 1

No primeiro teste em análise, usamos os equipamentos de cada aluno/utilizador, nomeadamente o seu computador portátil fazendo o arranque de CD-ROM e de USB *Pen Drive* com o sistema fornecido e previamente configurado para acesso ao SCENARIOS.

Para um total de 31 computadores e respetivos alunos, distribuídos pelos fabricantes ACER (6), ASUS (4), DELL (2), HP (7), IBM (2), SAMSUNG (3), SONY (2) e TOSHIBA (5). Uma vez que se tratam de equipamentos recentes, entre 0 e 2 anos de utilização, todos apresentavam características de processador, memória, disco, rede e gráfica que não condicionam as observações realizadas.

Para cada parâmetro observado registou-se a sua evolução durante o teste de utilização em intervalos de tempo regulares.

No arranque das observações, como se pode observar nos Gráficos 1, 2 e 3, verifica-se que a plataforma apresenta níveis estáveis e contínuos antes de se iniciar a utilização por parte dos alunos, como se pode observar nos gráficos dos parâmetros registados entre as 14:40 e as 15:10.

Gráfico 1 – Registo inicial da utilização da CPU

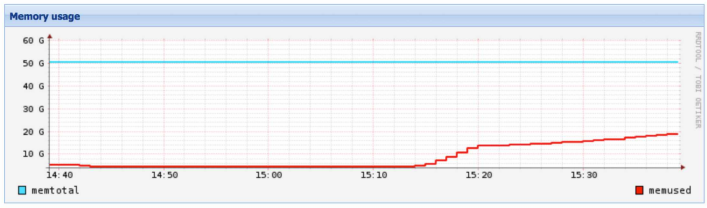


Gráfico 2 – Registo inicial da utilização da memória

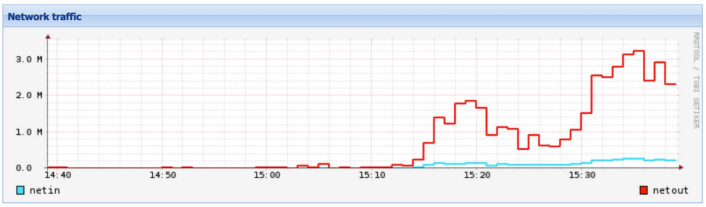


Gráfico 3 – Registo inicial da utilização da rede

No intervalo de preparação, 15:10/15:20, em que se verificam utilizadores, grupos e VMs, observa-se o aumento, ao nível do servidor da plataforma SCENARIOS, no processamento, memória RAM em utilização e tráfego de rede.

Estes valores observados, nos gráficos anteriores, estão relativamente baixos (por exemplo o tráfego de rede registado não chega aos 4 MBit, a memória e CPU estão bastante abaixo dos 50%) em relação aos máximos que os recursos do servidor permitem, o que permite concluir que a plataforma pode suportar maior número de utilizadores e VMs.

A partir das 15:30, altura em que os alunos começaram a utilização efetiva do cenário, verificam-se aumentos em todos os parâmetros, que correspondem à utilização das VMs por parte de cada aluno.

Como se pode observar nos gráficos seguintes, em que registamos os parâmetros em observação em diferentes alturas do exercício, os valores continuam a flutuar, de acordo com a utilização individual de cada máquina virtual, no entanto, não atingem valores limite que impliquem a necessidade de mais recursos ao nível do servidor da plataforma.

A utilização do CPU está sempre abaixo dos 50 %, como se observa no Gráfico 4.

Gráfico 4 - Registos de utilização da CPU durante a realização do teste 1

A memória RAM disponível, num total de 48GB, apenas são usados cerca de 22GB no máximo da utilização, conforme Gráfico 5.

Gráfico 5 - Registos de utilização da memória durante a realização do teste 1

Em relação ao tráfego de rede gerado, os valores apresentam-se igualmente com níveis baixos. De acordo com o Gráfico 6, o valor máximo registado é de 3,6 MBit, para uma rede a GBit, estando este registo numa ordem de grandeza abaixo.

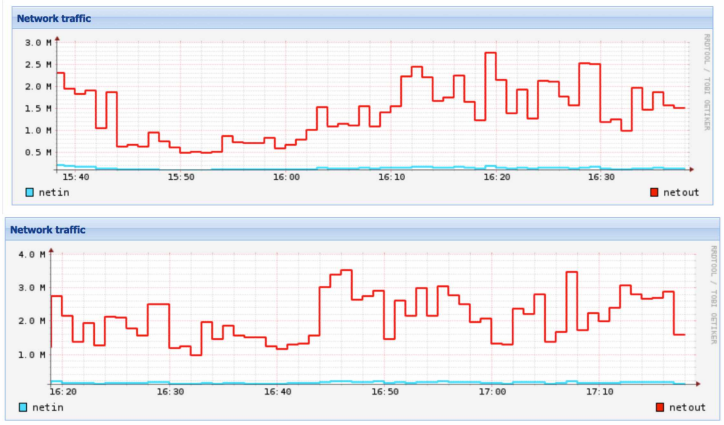


Gráfico 6 - Registos de utilização da rede durante a realização do teste 1

Os indicadores levam a concluir que podemos ter um número crescente de utilizadores e VMs, bem como cenários de utilização, sem que isso comprometa a rede, memória ou processamento do servidor.

7.1.2 Teste 2

No segundo teste de carga, usamos um conjunto de equipamentos afetos ao Laboratório UbiNET, do Instituto Politécnico de Beja, composto por 8 computadores de secretária, localizados na sala L11 da Escola Superior de Tecnologia e Gestão (ESTIG).

Estes equipamentos, apesar de mais antigos, apresentam características de hardware semelhantes e que não comprometem o seu desempenho na realização do teste.

Foram usados os CD-ROMs de *boot* criados para o acesso ao sistema de ensino, garantindo desta forma iguais condições de realização dos testes.

Um total de 8 alunos realizaram o teste, usando duas máquinas virtuais em simultâneo.

Em relação ao teste 1, diminuímos o número de alunos, e aumentámos a quantidade de VMs em utilização para duas por aluno.

Como podemos observar no Gráfico 7, a carga de utilização da CPU, para o tempo de espera não é relevante, estando abaixo dos 10% de utilização do processamento atribuído.

Gráfico 7 - Registos de utilização da CPU durante a realização do teste 2

Ao nível da utilização da memória verifica-se, pelo Gráfico 8, que esta apresenta um nível na ordem dos 10/12GB. Este indicador depende do tipo de cenário / tarefa que cada VM está a realizar, pelo que, face ao teste, está dentro dos valores espectáveis.

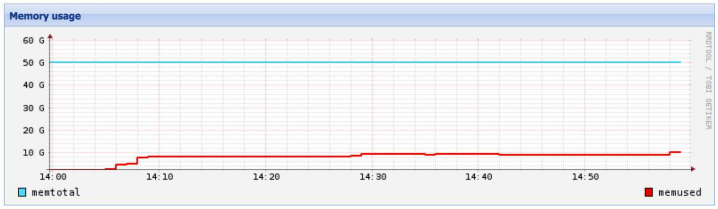


Gráfico 8 - Registos de utilização da memória durante a realização do teste 2

O tráfego de rede diminuiu face ao número de computadores a aceder ao sistema de ensino, passando para uma ordem de grandeza dos KBit. Conforme se observa no Gráfico 9, registou-se um valor máximo de 550KBit para o acesso dos 8 computadores, em termos de registo de saída de dados. O registo de `netin`, manteve a sua relação com o tráfego de saída.

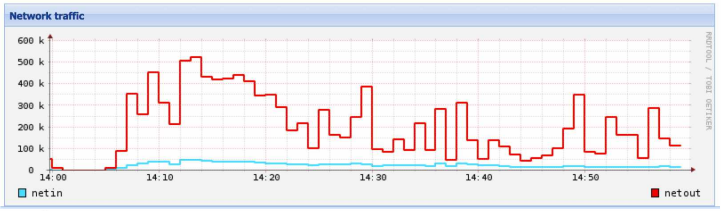


Gráfico 9 - Registos de utilização da rede durante a realização do teste 1

Como conclusão, o Teste 2 permitiu validar a possibilidade de utilização de computadores antigos para aceder à plataforma SCENARIOS com uma utilização normal em tudo semelhante à utilização recorrendo a computadores recentes como verificado no Teste 1.

Verificou-se também que a utilização de mais que uma máquina virtual por aluno não condicionou a utilização eficiente do sistema.

A utilização deste tipo de equipamentos permitiu ainda contornar a variedade de configurações necessárias, relativamente à utilização dos computadores pessoais

(portáteis) dos alunos do Teste 1, pois alguns portáteis não possuíam drive de CD/DVD e tinha que se iniciar de USB *Pen Drive*. Existem algumas condicionantes a alternar na BIOS que variam de marca para marca o que levou a algum tempo extra para o "setup" inicial de todos os alunos, que no Teste 2 não se verificou.

7.2 Usabilidade

Em termos de usabilidade, a plataforma de ensino SCENARIOS, apresenta uma interface que corresponde à da solução de virtualização que estamos a utilizar.

Nos testes de avaliação feitos com alunos, e, ao longo da sua utilização e configuração verificou-se que, em algumas áreas seria útil ter uma interface diferente, melhorada e com menos informação, para que a experiência fosse mais apelativa e, até, em alguns casos, mais objetiva do ponto de vista do ensino.

Desta forma, e porque à data deste trabalho não foi possível o seu desenvolvimento, remete-se para trabalhos futuros o desenvolvimento de uma solução de interface para a gestão e utilização da plataforma de ensino, de maneira que possa realçar os objetivos pedagógicos que se pretendem que a mesma atinja junto dos alunos. A solução de software implementada tem ao dispor uma API para que se possam desenvolver soluções à media.

CONCLUSÕES E TRABALHOS FUTUROS

Neste capítulo serão abordados os assuntos relacionados com as conclusões desta dissertação e possíveis melhoramentos e trabalhos a realizar no futuro.

8 Conclusões e Trabalhos Futuros

O estudo de uma plataforma de ensino, nos dias de hoje, tende a ser muito dinâmico, quer por haver necessidades que se vão alterando, quer pelos conteúdos específicos desta área que obrigam a uma adaptação quase constante. Neste sentido, pode-se afirmar que a plataforma SCENARIOS apresentada pode, no limite, estar sempre a ser melhorada.

A proposta de trabalho vem no seguimento dos objetivos que o Mestrado em Engenharia de Segurança Informática se propõe na sua vertente ofensiva. Ensinar técnicas de *hacking* na perspetiva de que ao conhecer o ataque e como se ataca, melhor se defende do ataque.

A plataforma SCENARIOS está alinhada com esses mesmos objetivos e procura cumprir o propósito para o qual foi pensada e criada: uma plataforma para o ensino em ambiente de laboratório virtualizado, baseada em tecnologias abertas e de baixo custo, orientada para o ensino de técnicas de *hacking* em conformidade com as taxonomias vigentes, através de um conjunto de conteúdos multimédia, estruturados de forma pedagógica centrada na aprendizagem pela prática, que possibilite inclusivamente o ensino à distância.

Para tal, analisaram-se as diferentes formações e certificações existentes, com e sem certificação, para melhor compreender o mercado empresarial neste setor, e assim procurar que a vertente pedagógica saísse enriquecida para cada aluno.

Propõe-se uma solução de virtualização, plataforma de ensino SCENARIOS, que suporta o ensino de técnicas de *hacking*, através da criação de ambientes e cenários que permitam aos alunos e professores explorar os sistemas, ferramentas, vulnerabilidades e *exploits*, orientada para o ensino. Esta orientação é sustentada com um conjunto de cenários de arquitetura que permitem, de forma faseada, a integração, implementação e crescimento da solução desde a sala de aula até ao ensino à distância.

Podendo adotar diferentes modelos, propõe-se, baseado nas referências taxionómicas existentes, o uso do CAPEC para a criação de um modelo para o ensino de técnicas de *hacking* com base no conhecimento dos ataques.

A plataforma SCENARIOS foi usada com alunos para verificações de carga ao servidor e para observação do seu uso efetivo. Destes testes retirou-se que os recursos existentes, ao nível do *hardware* e *software*, suportam a carga e preenchem os requisitos para a implementação e uso do sistema de ensino.

Sabendo-se que cada projeto tem sempre aspetos mais e menos conseguidos, e um trabalho desta natureza e dimensão, não está concluído em definitivo. Há e haverá, decorrentes de um trabalho e análise continuados, melhoramentos e novas necessidades a implementar, algumas das quais foram sendo identificadas e remetidas para trabalhos futuros.

No decorrer da sua conceção, criação, implementação, utilização, testes e avaliação, foram sendo feitos ajustes e melhoramentos, no entanto nem todos puderam ser desenvolvidos e/ou implementados ficando para trabalhos futuros. Ficam alguns que irão certamente melhorar a qualidade e funcionalidades da plataforma SCENARIOS, como por exemplo:

- Criação de uma interface de gestão e administração da plataforma;
- Criação de mais tarefas automatizadas, via scripts ou através de uma interface de parametrização de opções;
- Criação de uma rede de parceiros para a utilização e certificação de competências em segurança e cibersegurança da informação;

REFERÊNCIAS BIBLIOGRÁFICAS

Referências bibliográficas

[1] International Information System Security Certification Consortium, Inc., (ISC)²®. (2015, June) ISC2. [Online]. https://www.isc2.org/

[2] Offensive Security. Offensive Security Web Site. [Online]. http://www.offensive-security.com

[3] SANS. (2015, Apr.) SANS Technology Institute. [Online]. http://www.sans.org

[4] EC-Council. (2015, May) EC-Council web site. [Online]. http://www.eccouncil.org/

[5] KALI Linux. (2015, Apr.) KALI Linux Web Page. [Online]. http://www.kali.org

[6] Exploit Database. (2015, Apr.) Exploit DB. [Online]. http://www.exploit-db.com

[7] GIAC. (2015, Apr.) Global Information Assurance Certification. [Online]. http://www.giac.org

[8] VulHub. (2015, Mar.) [Online]. http://vulnhub.com

[9] HackingDojo. (2015, Mar.) [Online]. http://hackingdojo.com

[10] Smash the Stack. (2015, Mar.) [Online]. http://smashthestack.org

[11] Hack this Site. (2015, Mar.) [Online]. http://www.hackthissite.org

[12] Over the Wire. (2015, Mar.) [Online]. http://overthewire.org

[13] Moodle. (2015, Apr.) Moodle Web Site. [Online]. http://www.moodle.org

[14] VMWare. (2015, May) VMWare. [Online]. http://www.vmware.com

[15] Microsoft. (2015, May) Hyper-V Server. [Online]. http://www.microsoft.com/OEM/en/products/servers/Pages/hyper_v_server.aspx#fbid=jg3CXgiRe_E

[16] Citrix. (2015, June) XenServer. [Online]. http://www.citrix.com/products/xenserver/overview.html

[17] Proxmox VE. (2015, June) [Online]. http://www.proxmox.com

[18] Oracle. (2015, June) Virtual Box. [Online]. https://www.virtualbox.org/

[19] VMWare. (2015, July) VMWare web site. [Online]. https://www.vmware.com/pdf/vmware_player200.pdf

[20] VMWare. (2015, July) VMWare web site. [Online]. http://www.vmware.com/files/pdf/vsphere/VMW-vSPHR-Datasheet-6-0.pdf

[21] Microsoft. (2015, May) Hyper-V Server technet site. [Online]. https://technet.microsoft.com/en-us/library/hh831531.aspx

[22] Citrix. (2015, June) Citrix web site. [Online]. https://www.citrix.com/content/dam/citrix/en_us/documents/products-solutions/citrix-xenserver-industry-leading-open-source-platform-for-cost-effective-cloud-server-and-desktop-virtualization.pdf

[23] Wasim Ahmed, *Mastering Proxmox*.: Packet Publishing Ldt., 2014.

[24] ProxmoxVE. (2015, May) Proxmox web site. [Online]. http://www.proxmox.com/images/download/pve/docs/Proxmox-VE-Datasheet.pdf

[25] Oracle. (2015, May) VirtualBox web site. [Online]. http://www.oracle.com/us/technologies/virtualization/oraclevm/oracle-vm-virtualbox-ds-1655169.pdf

[26] Wasim Ahmed, "Dive into the Virtual World with Proxmox," in *Mastering Proxmox*.: Packet Publishing Ldt., 2014, pp. 6-43.

[27] Wasim Ahmed, "A Virtual Machine for a Virtual World," in *Mastering Proxmox*.: Packet Publishing, Ldt., 2014, pp. 96-110.

[28] MITRE - CVE. (2015, Apr.) Common Vulnerabilities and Exposures. [Online]. http://cve.mitre.org

[29] MITRE - CAPEC. (2014, May) Common Attack Pattern Enumeration and Classification. [Online]. http://capec.mitre.org

[30] European Parliament. (2004, March) Regulation (EC) No 460/2004 of the European Parliament and of the Coucil. [Online]. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004R0460:EN:HTML

[31] ENISA. (2015, May) European Union Agency for Network and Information Security. [Online]. http://www.enisa.europa.eu/

[32] NIST. (2015, May) National Institute of Standards and Techonology. [Online]. http://www.nist.gov/

[33] Carnegie Mellon University. (2015, June) CERT / CERT-CC. [Online]. http://www.cert.org/

[34] Centro Nacional de Ciberseguraça. (2015, July) CERT.PT. [Online]. http://www.cncs.gov.pt/cert-pt/index.html

[35] Centro Nacional de Cibersegurança. (2015, June) RFC2350 - CERT.PT. [Online]. http://www.cncs.gov.pt/media/2015/06/RFC2350_pt.txt

[36] MITRE. (2015, Apr.) MITRE Web Site. [Online]. http://www.mitre.org

[37] MITRE - CWE. (2015, Apr.) Common Weakness Enumeration. [Online]. http://cwe.mitre.org

[38] Simon Hansman, "A Taxonomy of Network and Computer Attack Methodologies," Department of Computer Science and Software Engineering, University of Canterbury, Christchurch, New Zealand, 2003.

[39] R. Bisbey and D. Hollingworth, "Protection Analysis: Final Report," University of Southern California, Technical Report 1978.

[40] R.P. Abbott et al., "Secutrity Analysis and Enhancements of Computer Operating Systems," Institute for Computer Sciences and Technology, Technical Report 1976.

[41] T. Aslam, A Taxonomy of Security Faults in the Unix Operating System, 1995.

[42] Matt Bishop, "A taxonomy of (unix) sistem and network vulnerabilities," Department of Computer Science, University of California, Technical Report 1995.

[43] Daniel L. Lough, A taxonomy of computer attacks with aplications to wireless networks, 2001.

[44] M. Bishop and D. Bailey, A critical analysis of vulnerability taxonomies, 1996.

[45] John D. Howard, An analysis of security incidents on the internet 1989-1995, 1997.

[46] Greg Hoglund and Gary McGraw, *Exploiting Software: How to Break Code*.: Addison-Wesley, 2004.

[47] MITRE. (2015, May) Making Security Measurable. [Online]. http://makingsecuritymeasurable.mitre.org/docs/capec-intro-handout.pdf

[48] Sean Barnum and Amit Sethi. (2013, May) Build Security In. [Online]. https://buildsecurityin.us-cert.gov/articles/knowledge/attack-patterns/introduction-to-attack-patterns

[49] MITRE. (2015, July) Documentos de suporte. [Online]. http://makingsecuritymeasurable.mitre.org/docs/capec-intro-handout.pdf

[50] MITRE. (2015, July) Common Vulnerabilities and Exposurs - Organizations/Contributions. [Online]. http://cve.mitre.org/compatible/organizations.html

[51] MITRE. (2015, July) Common Wekeaness Enumeration - Organizations/Contributions. [Online]. http://cwe.mitre.org/compatible/organizations.html

APÊNDICES

Apêndice 1 – Documento de apoio à configuração

Acesso à plataforma de ensino SCENARIOS

Apoio à Configuração

Para aceder à plataforma SCENARIOS tem de configurar o seu computador seguindo os passos indicados neste guião.

Passo1. Requisitos do sistema - computador do aluno e do professor - para aceder ao ambiente virtual de ensino:

i) estar na rede `192.168.69.0/24`
ii) ter instalado o *plugin java* para o seu *borwser* (verificar em `http://www.java.com`)
iii) na *Consola JAVA*, adicionar ao separador 'Segurança', as exceções: `https://192.168.69.150` e `https://192.168.69.150:8006`

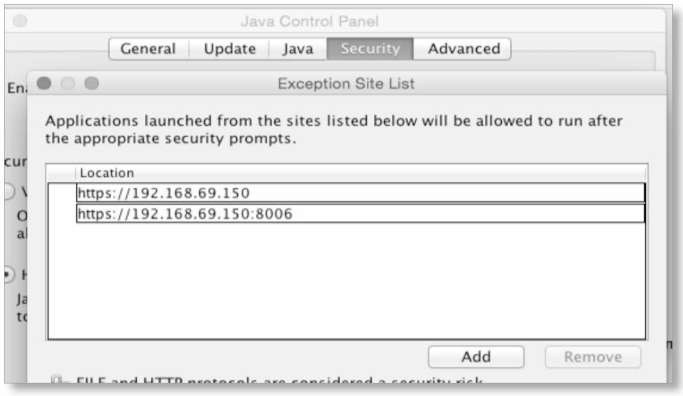


Figura 39 - Lista de exceções da *Consola JAVA*

Passo 2. Aceder ao servidor onde se encontra a plataforma de ensino SCENARIOS. Numa nova janela do seu *browser* aceda ao endereço `https://192.168.69.150:8006`

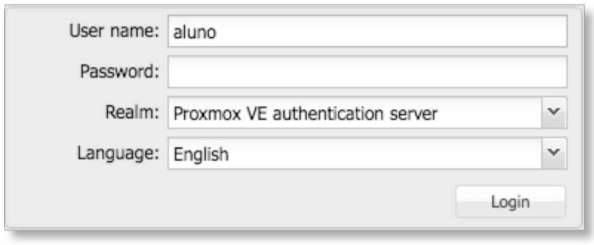


Figura 40 - Janela de acesso ao ambiente da plataforma

Passo 3. Utilize os dados de acesso que lhe foram atribuídos pelo professor – *User name* e *Password* – e clique em **Login** e de seguida em **OK** na janela de subscrição.

Nota #1: em `Realm`, escolha a primeira opção (`PVE authentication server`)

Nota #2: depois de fazer **Login**, pode alterar a sua *password* de utilizador em `Server View` > `Datacenter`, no separador **Users**, escolher o seu utilizador e clicar quem **Password**.

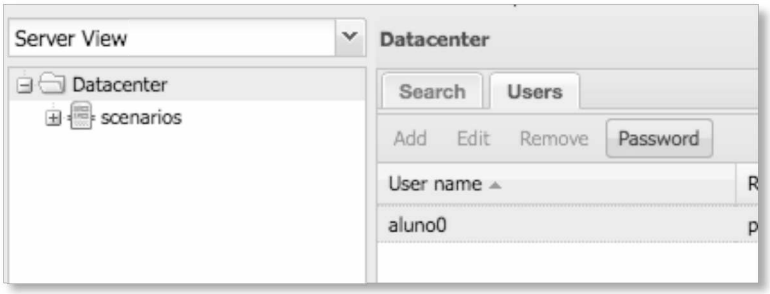


Figura 41 - Para alterar a password de utilizador

Passo 4. Para aceder às suas máquinas virtuais (VM), siga os passos mostrados da Figura 42 à Figura 45:

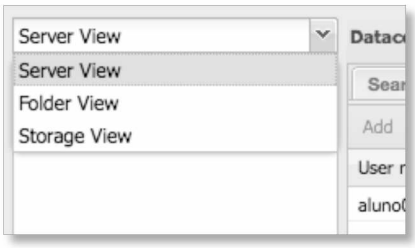


Figura 42 - Para aceder às suas VMs, escolha 'Server View' > 'Datacenter'

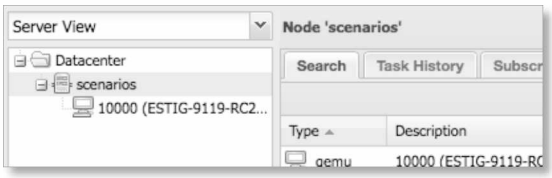


Figura 43 - Em 'scenarios' escolha a VM a que quer aceder

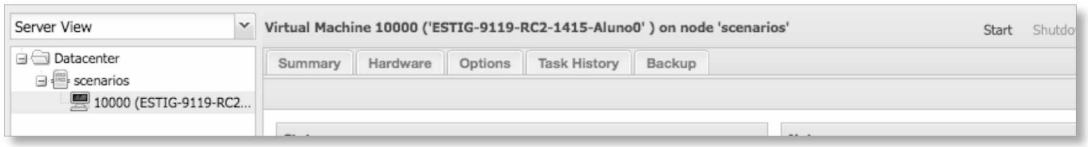


Figura 44 - Caso a VM não esteja ligada, clique em 'Start'

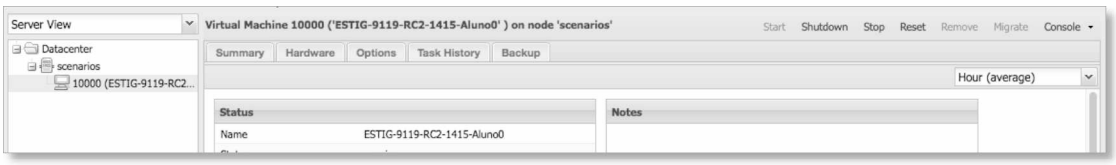


Figura 45 - Para aceder ao ecrã da VM clique em 'Console'

Passo 5. Acesso ao ambiente de trabalho – **Console** - de uma VM. Da Figura 46 à Figura 48.

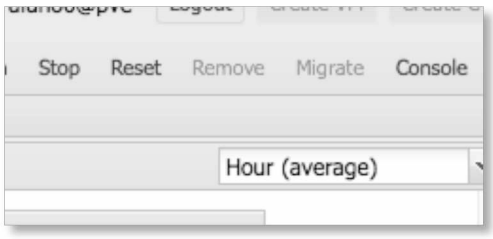


Figura 46 - Clique em 'Console' para aceder ao ambiente da VM

Figura 47 - Aviso de segurança. Clique 'Continuar'

Figura 48 - Aviso de segurança. Aceite e clique em 'Run'

Nota #3: Caso o servidor VNC leve algum tempo a responder, pode acontecer o erro ilustrado na figura. Clique em **Reload** e aguarde pelo ambiente de trabalho da VM a que pretende aceder (Figura 49).

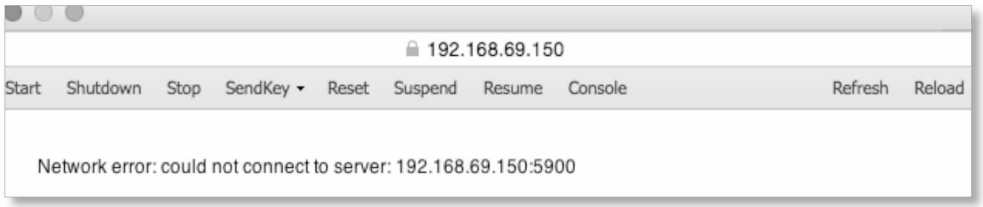


Figura 49 - Erro de 'time out' da VM

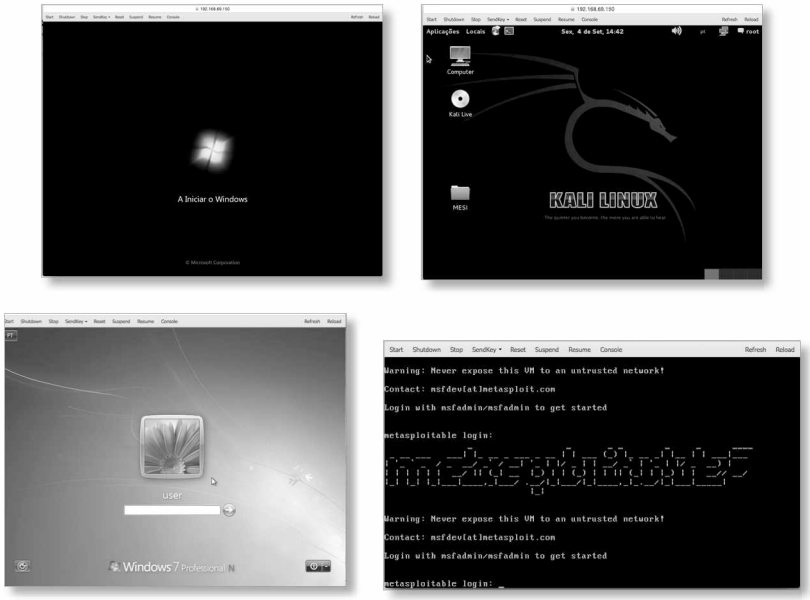


Figura 50 - Ambiente de trabalho - consola - de uma VM

Passo 6. Na janela de *login* das VMs (Figura 50), para aceder ao seu ambiente de trabalho utilize os dados indicados pelo professor.

Passo 7. Sair do ambiente de ensino. Feche todas as janelas das VMs e clique em **Logout** (Figura 51).

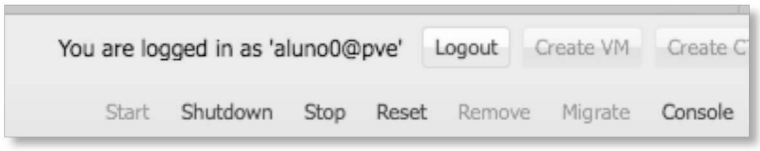


Figura 51 - Para sair clique em 'Logout'

Bom trabalho! ☺